

527,072

Reg'd PCT/PTO 09 MAR 2005

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年 4 月 1 日 (01.04.2004)

PCT

(10) 国際公開番号
WO 2004/028079 A1

- (51) 国際特許分類⁷: H04L 9/32, 9/08, G06F 15/00
- (21) 国際出願番号: PCT/JP2003/011802
- (22) 国際出願日: 2003 年 9 月 17 日 (17.09.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-273903 2002 年 9 月 19 日 (19.09.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 大森 和雄 (OMORI, Kazuo) [JP/JP]; 〒141-0001 東京都品川区

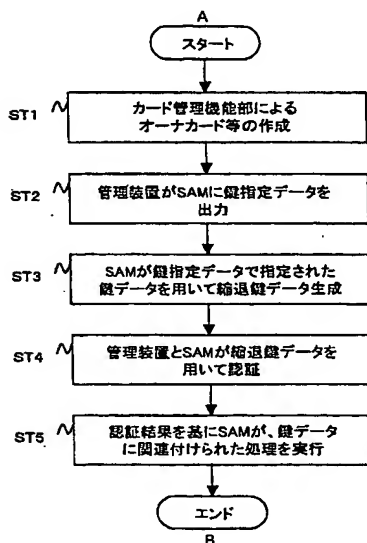
北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 本城 哲 (HONJO, Akira) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 末吉 正弘 (SUEYOSHI, Masahiro) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 花木 直文 (HANAKI, Naofumi) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 館野 啓 (TATENO, Kei) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).

- (74) 代理人: 佐藤 隆久 (SATO, Takahisa); 〒111-0052 東京都台東区柳橋 2 丁目 4 番 2 号 宮木ビル 4 階 創造国際特許事務所 Tokyo (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK,

[続葉有]

(54) Title: DATA PROCESSING METHOD, ITS PROGRAM AND ITS DEVICE

(54) 発明の名称: データ処理方法、そのプログラムおよびその装置



A...START
ST1...CARD MANAGEMENT FUNCTIONAL UNIT CREATES OWNER CARD.
ST2...MANAGEMENT DEVICE OUTPUTS KEY SPECIFICATION DATA TO SAM.
ST3...SAM GENERATES DEGENERATE KEY DATA USING KEY DATA SPECIFIED BY KEY SPECIFICATION DATA.
ST4...MANAGEMENT DEVICE AND SAM PERFORM AUTHENTICATION USING DEGENERATE KEY DATA.
ST5...SAM EXECUTES PROCESSING ASSOCIATED WITH KEY DATA ACCORDING TO AUTHENTICATION RESULT.
B...END

(57) Abstract: A management device (20) outputs key specification data, read from a card, to an SAM unit (9a). The SAM unit (9a) generates degenerate key data using two-way authentication key data specified by the key specification data. The management device (20) and the SAM unit (9a) perform authentication using the degenerate data. When the SAM unit (9a) authenticates the management device (20), the SAM unit (9a) executes a processing associated with one or more sets of two-way authentication key data used for generating the degenerate key data.

(57) 要約: 管理装置 20 が、カードから読み込んだ鍵指定データを SAM ユニットに 9a に出力する。SAM ユニット 9a が、鍵指定データが指定する相互認証鍵データを用いて縮退鍵データを生成する。管理装置 20 と SAM ユニット 9a とで縮退鍵データを用いて認証を行う。SAM ユニット 9a が管理装置 20 の正当性を認めると、上記縮退鍵データの生成に用いられた単数または複数の相互認証鍵データに関連付けられた処理を実行する。

WO 2004/028079 A1



DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

- (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,

GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

データ処理方法、そのプログラムおよびその装置

5 技術分野

本発明は、認証結果を基に所定の処理を行うデータ処理方法、そのプログラムおよびその装置に関する。

背景技術

- 10 認証元（認証手段）が、認証先（被認証手段）の正当性を確認した後に、当該認証先に許可された処理を実行するシステムがある。

このようなシステムでは、例えば、認証元が、全ての認証先についての相互認証鍵データを保持し、それぞれの認証元との間で、当該認証元に対応する相互認証鍵データを選択して相互認証を行う。

- 15 そして、認証元は、上記相互認証により、認証先の正当性を確認すると、管理テーブルなどを基に予め認証先に対して許可された処理を特定し、当該特定した処理を実行する。

しかしながら、上述した従来のシステムでは、認証先は、全ての認証元に対応した相互認証鍵データを保持する必要がある、相互認証鍵データの管理負担が大

- 20 きいという問題がある。

また、上述した従来のシステムでは、相互認証とは別に、認証先に許可した処理を管理テーブルを基に特定する必要がある、管理テーブルの作成および管理などの負担が大きいという問題がある。

25 発明の開示

本発明は、認証手段が被認証手段を認証した後に、当該被認証手段に許可した処

理を実行する場合に、認証手段の処理負担を軽減することを可能にするデータ処理方法、そのプログラムおよびその装置を提供することを目的とする。

上述した目的を達成するために、第1の発明のデータ処理方法は、鍵データを用いて暗号化を行って生成された第1の認証用データを保持する被認証手段と、

- 5 前記鍵データを保持する認証手段とが行うデータ処理方法であって、前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手段に提供する第1の工程と、前記認証手段が、前記第1の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記暗号化を行って第2の認証用データを生成する第2の工程と、前記被認証手段が前記第1の認証用データを用い、前記認証手段が前記
- 10 第2の認証用データを用いて、認証を行う第3の工程と、前記認証手段が、前記第3の工程の前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断すると、前記鍵データに関連付けられた処理を実行する第4の工程とを有する。

第1の発明のデータ処理方法の作用は以下になる。

- 15 第1の工程において、前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手段に提供する。

次に、第2の工程において、前記認証手段が、前記第1の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記暗号化を行って第2の認証用データを生成する。

- 20 次に、第3の工程において、前記被認証手段が前記第1の認証用データを用い、前記認証手段が前記第2の認証用データを用いて、認証を行う。

次に、第4の工程において、前記認証手段が、前記第3の工程の前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断すると、前記鍵データに関連付けられた処理を実行する。

- 25 第2の発明のデータ処理システムは、鍵データを用いて暗号化を行って生成された第1の認証用データを保持する被認証手段と、前記鍵データを保持する認証

手段とを有し、前記被認証手段が、前記鍵データを指定する鍵指定データを前記
認証手段に提供し、前記認証手段が、前記被認証手段から受けた前記鍵指定デー
タが指定する前記鍵データを用いて暗号化を行って第2の認証用データを生成し、
前記被認証手段が前記第1の認証用データを用い、前記認証手段が前記第2の認
5 証用データを用いて、認証を行い、前記認証手段が、前記認証により、前記第1
の認証用データと前記第2の認証用データとが同じであると判断すると、前記鍵
データに関連付けられた処理を実行する。

第2の発明のデータ処理システムの作用は以下のようになる。

10 先ず、前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手
段に提供する。

次に、前記認証手段が、前記第1の工程で受けた前記鍵指定データが指定する
前記鍵データを用いて前記暗号化を行って第2の認証用データを生成する。

次に、前記被認証手段が前記第1の認証用データを用い、前記認証手段が前記
第2の認証用データを用いて、認証を行う。

15 次に、前記認証手段が、前記認証により、前記第1の認証用データと前記第2
の認証用データとが同じであると判断すると、前記鍵データに関連付けられた処
理を実行する。

第3の発明のデータ処理方法は、所定の鍵データを保持する認証手段が、前記
鍵データを用いて暗号化を行って生成された第1の認証用データを保持する被認
20 証手段と認証を行うデータ処理方法であって、前記鍵データを指定する鍵指定デ
ータを前記被認証手段から受ける第1の工程と、前記第1の工程で受けた前記鍵
指定データが指定する前記鍵データを用いて前記暗号化を行って第2の認証用デ
ータを生成する第2の工程と、前記第2の工程で生成した前記第2の認証用デー
タを用いて、前記第1の認証用データを認証に用いる前記被認証手段と前記認証
25 を行う第3の工程と、前記第3の工程の前記認証により、前記第1の認証用デー
タと前記第2の認証用データとが同じであると判断した場合に、前記鍵データに

関連付けられた処理を実行する第4の工程とを有する。

第4の発明のデータ処理装置は、所定の鍵データを用いて暗号化を行って生成された第1の認証用データを保持する被認証手段と認証を行い、前記鍵データを保持するデータ処理装置であって、前記被認証手段から、前記鍵データを指定する鍵指定データを入力する入力手段と、前記入力手段が受けた前記鍵指定データが指定する前記鍵データを用いて前記暗号化を行って第2の認証用データを生成し、当該第2の認証用データを用いて、前記第1の認証用データを認証に用いる前記被認証手段と前記認証を行う認証手段と、前記認証手段が前記認証により前記第1の認証用データと前記第2の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処理を実行する制御手段とを有する。

第5の発明のプログラムは、所定の鍵データを用いて暗号化を行って生成された第1の認証用データを保持する被認証手段と認証を行い、前記所定の鍵データを保持するデータ処理装置が実行するプログラムであって、前記鍵データを指定する鍵指定データを前記被認証手段から受ける第1の手順と、前記第1の手順で受けた前記鍵指定データが指定する前記鍵データを用いて前記暗号化を行って第2の認証用データを生成する第2の手順と、前記第2の手順で生成した前記第2の認証用データを用いて、前記第1の認証用データを認証に用いる前記被認証手段と前記認証を行う第3の手順と、前記第3の手順の前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処理を実行する第4の手順とを有する。

第6の発明のデータ処理方法は、鍵データを保持する認証手段が、第1の認証用データを保持する被認証手段から指定された前記鍵データを用いて暗号化を行って第2の認証用データを生成し、前記第2の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第1の認証用データと前記第2の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、前記被認証手段が行うデータ処理方法であって、前記

所定の生成方法を基に前記第 1 の認証用データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の工程と、前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2 の工程と、前記第 2 の工程の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第 3 の工程とを有する。

第 7 の発明のデータ処理装置は、鍵データを保持する認証手段が、第 1 の認証用データを保持する被認証手段から指定された前記鍵データを用いて暗号化を行って第 2 の認証用データを生成し、前記第 2 の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、前記被認証手段を構成するデータ処理装置であって、前記所定の生成方法を基に前記第 1 の認証用データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の手段と、前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2 の手段と、前記第 2 の手段の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第 3 の手段とを有する。

第 8 の発明のプログラムは、鍵データを保持する認証手段が、第 1 の認証用データを保持する被認証手段から指定された前記鍵データを用いて暗号化を行って第 2 の認証用データを生成し、前記第 2 の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、前記被認証手段を構成するデータ処理装置によって実行されるプログラムであって、前記所定の生成方法を基に前記第 1 の認証用データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の手順と、前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2 の手順と、前記第 2 の手順の認証の結果を基に、前記鍵データに関

連付けられた処理を前記認証手段に行わせる第3の手順とを有する。

図面の簡単な説明

図1は、本発明の実施形態の通信システムの全体構成図である。

5 図2は、図1に示す管理装置の機能ブロック図である。

図3は、図2に示す管理装置が行う処理手順の概要を説明するためのフローチャートである。

図4は、図2に示すAP編集ツールおよび管理ツールに係わる処理において用いられるカードを説明するための図である。

10 図5は、図1に示すICカードの機能ブロック図である。

図6は、図5に示すメモリに記憶されたデータを説明するための図である。

図7は、図1に示すSAMモジュールのソフトウェア構成を説明するための図である。

15 図8は、図1に示すSAMモジュールのハードウェア構成、並びに外部メモリ7の記憶領域を説明するための図である。

図9は、図8に示すAP記憶領域を説明するための図である。

図10は、アプリケーションエレメントデータを説明するための図である。

図11は、アプリケーションエレメントデータAPEのタイプを説明するための図である。

20 図12は、オナーカードおよびユーザカードの作成手順を説明するためのフローチャートである。

図13は、相互認証鍵データを説明するための図である。

図14は、相互認証コードを説明するための図である。

図15は、相互認証鍵データとサービスとの関係を説明するための図である。

25 図16は、縮退鍵データの生成方法を説明するための図である。

図17は、縮退鍵データのその他の生成方法を説明するための図である。

図18は、縮退鍵データの暗号化の階層を説明するための図である。

図19は、縮退鍵データの特性の一例を説明するための図である。

図20は、相互認証鍵データの使用形態の一例を説明するための図である。

図21は、図1に示す管理装置のSAM管理機能部とSAMユニットとの間の
5 相互認証について説明するためのフローチャートである。

図22は、図1に示す管理装置のSAM管理機能部とSAMユニットとの間の
相互認証について説明するための図21の続きのフローチャートである。

図23は、SAMユニットの処理を説明するためのフローチャートである。

図24は、図2および図4を用いて説明した管理装置に関する各種のカード
10 の発行に用いられる画面を説明するための図である。

図25は、オナカードの作成用画面を説明するための図である。

図26は、カード要求画面を説明するための図である。

図27は、ユーザカードの作成用画面を説明するための図である。

図28は、AP暗号化カードの作成用画面を説明するための図である。

15 図29は、トランスポートカードの作成用画面を説明するための図である。

図30は、SAM管理画面を説明するための図である。

図31は、図30に示すSAMツリー領域の表示内容の一例を示す画面を説明
するための図である。

図32は、図30に示すSAMツリー領域に表示されるアイコンを説明するた
20 めの図である。

図33は、SAMネットワーク画面を説明するための図である。

図34は、グループ画面を説明するための図である。

図35は、SAM画面を説明するための図である。

図36は、AP記憶領域画面を説明するための図である。

25 図37は、APEタイプ画面を説明するための図である。

図38は、インスタンス画面を説明するための図である。

図39は、図30に示すメニュー・バーのSAMコマンドを指定した場合の画面である。

図40は、図30に示すSAM管理画面上でSAMのグループを作成する場合を説明するための図である。

5 図41は、AP記憶領域エディタ画面を説明するための図である。

図42は、アプリケーションエレメントデータAPEのパッケージの追加を行うための画面を説明するための図である。

図43は、アプリケーションエレメントデータAPEの作成を行うための画面を説明するための図である。

10 図44は、アプリケーションエレメントデータAPEのバージョン追加を行うための画面を説明するための図である。

図45は、一連の処理を経た後のAP記憶領域エディタ画面を説明するための図である。

15 発明を実施するための最良の形態

これより図面を参照して本発明の好適実施例について説明していく。

図1は、本実施形態の通信システム1の全体構成図である。

図1に示すように、通信システム1は、店舗などに設置されたサーバ装置2、ICカード3、カードリーダー・ライタ4、パーソナルコンピュータ5、ASP
20 (Application Service Provider)サーバ装置19、SAM(Secure Application Module)ユニット9a, 9b,...、管理装置20、ICモジュール42が内蔵された携帯通信装置41を用いて、インターネット10を介して通信を行ってICカード3あるいは携帯通信装置41を用いた決済処理などの手続き処理を行う。

通信システム1では、管理装置20およびSAMユニット9a, 9bが本発明
25 に対応した実施の形態に係わる処理を行う。

すなわち、管理装置20は、管理者等によって許可された所定の処理をSAM

ユニット 9 a, 9 bに行わせるために用いる I C (本発明の集積回路) を内蔵したカード (例えば、後述するオナカードおよびユーザカード) を発行する処理を行う。これにより、相互認証に必要なデータを被認証手段に対して提供する。

また、管理装置 2 0 は、上記発行されたカードを管理者やユーザが用いて、S
5 AMユニット 9 a, 9 bとの間で相互認証を行い、上記許可された所定の処理を SAMユニット 9 a, 9 bに行わせる。

この場合に、管理装置 2 0 が本発明の被認証手段となり、S AMユニット 9 a, 9 bが本発明の認証手段となる。

図 2 は、管理装置 2 0 の機能ブロック図である。

10 図 2 に示すように、管理装置 2 0 は、例えば、A P編集ツール 5 1、管理ツール 5 2、カードリーダー・ライター 5 3、ディスプレイ 5 4、I / F 5 5 および操作部 5 6 を有する。

ここで、管理装置 2 0 が、第 8 の発明のデータ処理装置に対応し、I / F 5 5
は本発明の第 1 の手段、S AM管理機能部 5 7 が本発明の第 2 の手段および第 3
15 の手段に対応している。

A P編集ツール 5 1 および管理ツール 5 2 は、データ処理装置でプログラム(第 9 の発明のプログラムに対応)を実行して実現してもよいし、電子回路(ハードウェア)によって実現してもよい。

管理ツール 5 2 は、例えば、S AM管理機能部 5 7 およびカード管理機能部 5
20 8 を有する。

カードリーダー・ライター 5 3 は、以下に示す種々のカードの I C との間で、非接触式あるいは接触式でデータの授受を行う。

ディスプレイ 5 4 は、カード発行画面や A P 管理画面を表示するために用いられる。

25 I / F 5 5 は、S AMユニット 9 a, 9 b との間で、非接触式あるいは接触式でデータの授受を行う。

操作部 56 は、AP 編集ツール 51 および管理ツール 52 に対して、指示やデータを入力ために用いられる。

図 3 は、管理装置 20 が行う処理手順の概要を説明するためのフローチャートである。

5 ステップ ST1 :

管理装置 20 は、管理者の操作に応じて、カード管理機能部 58 により、カードリーダ・ライタ 53 にセットされたデフォルトカード 71 を用いて、所定のデータが格納されたオーナーカード 72 を作成する。また、オーナーカード 72 を用いてユーザカード 73 を作成する。

- 10 すなわち、管理装置 20 は、SAM ユニット 9a, 9b (本発明の認証手段) に係わる処理のうち、オーナーカード 72 およびユーザカード 73 を用いた被認証手段に許可する処理に関連付けられた相互認証鍵データ (本発明の鍵データ) を用いて、後述するデバイス鍵データを所定の暗号化方法 (本発明の所定の生成方法) で暗号化して、上記相互認証鍵データを復元困難な縮退鍵データ (本発明の
- 15 第 1 の認証用データ) を生成する。

そして、管理装置 20 は、上記生成した縮退鍵データと、当該縮退鍵データの生成に用いた上記相互認証鍵データを指定する鍵指定データとを、オーナーカード 72 およびユーザカード 73 の IC (本発明の集積回路) に書き込む。

- また、同様に、管理装置 20 は、トランスポートカード 74 および AP 暗号化
- 20 カード 75 を作成する。

ステップ ST2 :

オーナーカード 72 またはユーザカード 73 の使用者が、これらのカードを用いて、管理装置 20 を介して、当該使用者に権限が与えられた処理を SAM ユニット 9a, 9b に行わせる場合に、上記使用者が管理装置 20 のカードリーダ・ライタ 53 に、オーナーカード 72 またはユーザカード 73 の IC に記憶された上記

25 鍵指定データを読み込ませる。

管理装置 20 の SAM 管理機能部 57 は、当該読み込んだ鍵指定データを SAM ユニット 9 a, 9 b に出力する。

ステップ S T 3 :

5 SAM ユニット 9 a, 9 b が、上記鍵指定データが指定する相互認証鍵データを用いて、上記デバイス鍵データを上記所定の暗号化方法で暗号化して縮退鍵データ（本発明の第 2 の認証用データ）を生成する。

ステップ S T 4 :

10 SAM 管理機能部 57 がカード 7 2 または 7 3 から読み出した縮退鍵データを用い、SAM ユニット 9 a, 9 b が上記生成した縮退鍵データを用いて、認証を行う。

ステップ S T 5 :

15 SAM ユニット 9 a, 9 b が、上記認証により、SAM 管理機能部 57 と SAM ユニット 9 a, 9 b とが同じ上記縮退鍵データを保持していると判断すると、管理装置 20 からの指示に応じて、上記縮退鍵データの生成に用いられた単数または複数の相互認証鍵データに関連付けられた処理を実行する。

図 4 は、図 2 に示す AP 編集ツール 5 1 および管理ツール 5 2 に係わる処理において用いられるカードを説明するための図である。

20 図 4 に示すように、管理装置 20 の管理ツール 5 2 を用いて、SAM ユニット 9 a, 9 b にアクセスする場合に、オーナーカード 7 2 およびユーザカード 7 3 が用いられる。

また、AP 編集ツール 5 1 で生成した AP パッケージファイルを管理ツール 5 2 に提供する場合に、AP 暗号化カード 7 5 の IC に記憶された暗号化鍵データを用いて、当該 AP パッケージファイルが暗号化される。

すなわち、図 4 に示すように、ユーザが、AP 編集ツール 5 1 を用いて、SAM
25 M モジュール 8 内のアプリケーションプログラム AP を構成するアプリケーションエレメントデータ A P E を作成する。

そして、AP編集ツール51が、単数または複数のアプリケーションエレメントデータAPEを含むAPパッケージファイルを作成し、これをAP暗号化カード75に格納された暗号鍵データを用いて暗号化して管理ツール52に提供する。

管理ツール52は、上述したように、SAMユニット9a、9bと相互認証を行い、当該相互認証に用いた相互認証鍵データに関連付けて許可されたSAMユニット9a、9b内のAP記憶領域に対して、AP編集ツール51から受けたAPパッケージファイルを書き込む。

また、トランスポートカード74は、SAMユニット9a、9bが保持する鍵データなどのセキュリティに係わるデータを取り出して他の機器に転送したり、保存等するために用いられる。

〔ICカード3および携帯通信装置41〕

図5は、ICカード3の機能ブロック図である。

図5に示すように、ICカード3は、メモリ50およびCPU51を備えたIC(Integrated Circuit)モジュール3aを有する。

メモリ50は、図6に示すように、クレジットカード会社などのサービス事業者15__1が使用する記憶領域55__1、サービス事業者15__2が使用する記憶領域55__2、並びにサービス事業者15__3が使用する記憶領域55__3を有する。

また、メモリ50は、記憶領域55__1へのアクセス権限を判断するために用いられる鍵データ、記憶領域55__2へのアクセス権限を判断するために用いられる鍵データ、並びに記憶領域55__3へのアクセス権限を判断するために用いられる鍵データを記憶している。当該鍵データは、相互認証や、データの暗号化および復号などに用いられる。

また、メモリ50は、ICカード3あるいはICカード3のユーザの識別データを記憶している。

携帯通信装置41は、携帯電話網およびインターネット10を介してASPサ

一バ装置 19 a, 19 b と通信を行う通信処理部 43 と、通信処理部 43 との間でデータ授受可能な IC モジュール 42 とを有し、アンテナからインターネット 10 を介して SAM ユニット 9 a と通信を行う。

IC モジュール 42 は、携帯通信装置 41 の通信処理部 43 とデータ授受を行う点を除いて、前述した IC カード 3 の IC モジュール 3 a と同じ機能を有している。

なお、携帯通信装置 41 を用いた処理は、IC カード 3 を用いた処理と同様に行われ、IC モジュール 42 を用いた処理は IC モジュール 3 a を用いた処理と同様に行われるため、以下の説明では、IC カード 3 および IC モジュール 3 a を用いた処理について例示する。

以下、SAM ユニット 9 a, 9 b について説明する。

図 1 に示すように、SAM ユニット 9 a, 9 b は、外部メモリ 7 と SAM モジュール 8 とを有する。

ここで、SAM モジュール 8 は、半導体回路として実現してもよいし、筐体内に複数の回路を収容した装置として実現してもよい。

〔SAM モジュール 8 のソフトウェア構成〕

SAM モジュール 8 は、図 7 に示すようなソフトウェア構成を有している。

図 7 に示すように、SAM モジュール 8 は、下層から上層に向けて、ハードウェア HW 層、周辺 HW に対応した RTOS カーネルなどを含めたドライバ層 (OS 層)、論理的にまとまった単位の処理を行う下位ハンドラ層、アプリケーション固有のライブラリなどをまとめた上位ハンドラ層および AP 層を順に有している。

ここで、AP 層では、図 1 に示すクレジットカード会社などのサービス事業者 15__1, 15__2, 15__3 による IC カード 3 を用いた手続きを規定したアプリケーションプログラム AP__1, AP__2, AP__3 が、外部メモリ 7 から読み出されて動作している。

AP 層では、アプリケーションプログラム AP__1, AP__2, AP__3 相互

間、並びに上位ハンドラ層との間にファイアウォールFWが設けられている。

〔SAMモジュール8のハードウェア構成〕

図8は、SAMモジュール8のハードウェア構成、並びに外部メモリ7の記憶領域を説明するための図である。

- 5 図8に示すように、SAMモジュール8は、例えば、メモリI/F61、外部I/F62、メモリ63、認証部64およびCPU65を有し、これらがバス60を介して接続されている。

- ここで、SAMモジュール8が、第4の発明のデータ処理装置に対応し、外部I/F62が本発明の入力手段、認証部64が本発明の認証手段、CPU65が
10 本発明の制御手段にそれぞれ対応している。

また、SAMモジュール8が、第5の発明のデータ処理装置に対応し、以下に示す各手順を含むプログラムを実行して、その機能を実現してもよい。

メモリI/F61は、外部メモリ7との間でデータ授受を行う。

- 外部I/F62は、図1に示すASPサーバ装置19a、19bおよび管理装
15 置20との間で、データおよびコマンドの授受を行う。

メモリ63は、後述するSAMユニット9a、9bの相互認証などに用いられる種々の鍵データなどを記憶する。当該鍵データは、外部メモリ7のAP管理用記憶領域221に記憶されていてもよい。

- 認証部64は、後述する相互認証に係わる処理を行う。認証部64は、例えば、
20 所定の鍵データを用いた暗号化および復号などを処理を行う。

CPU65は、SAMモジュール8の処理を統括して制御する。

CPU65は、後述するように、相互認証で正当な相手であることを確認すると、被認証手段に対して、後述する相互認証鍵データに関連付けられた処理を許可し、これを実行する。

- 25 SAMモジュール8による相互認証処理については、後に詳細に説明する。

〔外部メモリ7〕

図8に示すように、外部メモリ7の記憶領域には、サービス事業者15__1のアプリケーションプログラムAP__1が記憶されるAP記憶領域220__1（サービスAPリソース領域）、サービス事業者15__2のアプリケーションプログラムAP__2が記憶されるAP記憶領域220__2、サービス事業者15__3のアプリケーションプログラムAP__3が記憶されるAP記憶領域220__3、並びにSAMモジュール208の管理者が使用するAP管理用記憶領域221（シスエムAPリソース領域および製造者APリソース領域）がある。

AP記憶領域220__1に記憶されているアプリケーションプログラムAP__1は、図9に示すように、後述する複数のアプリケーションエレメントデータAPE（本発明のデータモジュール）によって構成されている。AP記憶領域220__1へのアクセスは、ファイアウォールFW__1によって制限されている。

AP記憶領域220__2に記憶されているアプリケーションプログラムAP__2は、図9に示すように、複数のアプリケーションエレメントデータAPEによって構成されている。AP記憶領域220__2へのアクセスは、ファイアウォールFW__2によって制限されている。

AP記憶領域220__3に記憶されているアプリケーションプログラムAP__3は、図9に示すように、複数のアプリケーションエレメントデータAPEによって構成されている。AP記憶領域220__3へのアクセスは、ファイアウォールFW__3（図8に図示）によって制限されている。

本実施形態では、上記アプリケーションエレメントデータAPEは、例えば、SAMユニット9aの外部から外部メモリ7にダウンロードされる最小単位である。各アプリケーションプログラムを構成するアプリケーションエレメントデータAPEの数は、対応するサービス事業者が任意に決定できる。

また、アプリケーションプログラムAP__1、AP__2、AP__3は、例えば、それぞれ図1に示すパーソナルコンピュータ15__1、15__2、15__3を用いて、サービス事業者16__1、16__2、16__3によって作成され、SAM

モジュール 8 を介して外部メモリ 7 にダウンロードされる。

なお、AP 管理用記憶領域 221 に記憶されたプログラム、並びにデータも、上述したアプリケーションエレメントデータ APE を用いて構成されている。

図 10 は、上述したアプリケーションエレメントデータ APE を説明するため
5 の図である。

アプリケーションエレメントデータ APE は、図 10 に示すように、APE の属性（種別）を基に規定された分類を示す APE タイプによって規定されたインスタンスを用いて構成される。

各インスタンスは、エレメント ID と、エレメントプロパティと、エレメント
10 バージョンとによって規定されている。

APE タイプを基に、当該アプリケーションエレメントデータ APE が、サービス AP 記憶領域 220__1, 220__2, 220__3 および AP 管理用記憶領域 221 の何れに格納されるかが規定される。

サービス AP 記憶領域 220__1 は、各サービス事業者がアクセス可能なデータ
15 を記憶する。

なお、AP 管理用記憶領域 221 は、システムの管理者がアクセス可能なデータを記憶するシステム AP 記憶領域と、システムの製造者がアクセス可能なデータを記憶する製造者 AP 記憶領域とを有する。

また、サービス AP 記憶領域 220__1, 220__2, 220__3 および AP
20 管理用記憶領域 221 によって、AP 記憶領域が構成される。

本実施形態では、上述したサービス AP 記憶領域 220__1, 220__2, 220__3 および AP 管理用記憶領域 221 の各々には ID（AP 記憶領域 ID）が割り当てられており、APE タイプ、インスタンス、並びにエレメントバージョンの各々には識別用の番号（APE タイプ番号、インスタンス番号、並びにエレメントバージョン番号）が割り当てられている。
25

図 11 は、APE タイプの一例を説明するための図である。

図11に示すように、APEタイプには、ICシステム鍵データ、ICエリア
鍵データ、ICサービス鍵データ、IC縮退鍵データ、IC鍵変更パッケージ、
IC発行鍵パッケージ、IC拡張発行鍵パッケージ、ICエリア登録鍵パッケー
ジ、ICエリア削除鍵パッケージ、ICサービス登録鍵パッケージ、ICサービ
5 ス削除鍵パッケージ、ICメモリ分割鍵パッケージ、ICメモリ分割素鍵パッケー
ジ、障害記録ファイル、相互認証用鍵、パッケージ鍵、ネガリストおよびサー
ビスデータテンポラリファイルがある。

各APEタイプには、APEタイプ番号が割り当てられている。

以下、図11に示すAPEタイプのうち一部を説明する。

- 10 ICシステム鍵データ、ICエリア鍵データ、ICサービス鍵データおよびIC
縮退鍵データは、ICカード3およびICモジュール42のメモリ50に対し
てのデータの読み書き操作に用いられるカードアクセス鍵データである。

- 相互認証用鍵データ同一SAM内にあるAP間相互認証にも使用される。SA
M相互認証用鍵データとは、対応するアプリケーションエレメントデータAPE
15 を同一SAM内の他のAPまたは他のSAMからアクセスする際に用いられる鍵
データである。

ICメモリ分割用鍵パッケージは、サービス事業者がICカード3を用いたサ
ービスの運用開始前に、外部メモリ7やICカード3のメモリの記憶領域を分割
するために使用するデータである。

- 20 ICエリア登録鍵パッケージは、サービス事業者がICカード3を用いたサ
ービスの運用開始前に、ICカード3のメモリの記憶領域にエリア登録を行う場合
に使用するデータである。

ICエリア削除用鍵パッケージは、カードアクセス鍵データからSAM内部で
自動生成が可能なパッケージである。

- 25 ICサービス登録用鍵パッケージは、サービス事業者がICカード3を用いた
サービスの運用開始前に、外部メモリ7のアプリケーションエレメントデータA

P Eを登録するために用いられる。

I Cサービス削除用鍵パッケージは、外部メモリ 7 に登録されているアプリケーションエレメントデータ A P E を削除するために用いられる。

〔オーナーカード 7 2 およびユーザカード 7 3 の作成〕

- 5 図 1 2 は、オーナーカード 7 2 およびユーザカード 7 3 の作成手順を説明するためのフローチャートである。

図 1 2 は、図 3 に示すステップ S T 1 , S T 2 を詳細に示すものである。

ステップ S T 1 1 :

- 10 例えば、管理者が、オーナーカード 7 2 を作成する場合には、オーナーカード 7 2 の使用者に許可する S A M ユニット 9 a , 9 b に係わる処理を選択する。

また、管理者等が、ユーザカード 7 3 を作成する場合に、ユーザカード 7 3 の使用者に許可する S A M ユニット 9 a , 9 b に係わる処理を選択する。

- 15 S A M ユニット 9 a , 9 b に係わる処理には、例えば、S A M ユニット 9 a , 9 b が提供する機能を実行する処理、または S A M ユニット 9 a , 9 b が保持するデータ（例えば、アプリケーションエレメントデータ A P E ）へのアクセスなどがある。

ステップ S T 1 2 :

管理者等が、ステップ S T 1 1 で選択した処理に関連付けられた相互認証鍵データを選択して、管理装置 2 0 のカード管理機能部 5 8 に入力あるいは指定する。

- 20 当該相互認証鍵データについては後に詳細に説明する。

ステップ S T 1 3 :

管理装置 2 0 のカード管理機能部 5 8 が、ステップ S T 1 2 で選択された単数または複数の相互認証鍵データを用いて後述する縮退処理方法（本発明の所定の生成方法）を基に縮退鍵データを生成する。

- 25 当該縮退処理については後に詳細に説明する。

ステップ S T 1 4 :

管理装置 20 のカード管理機能部 58 が、ステップ S T 13 で縮退鍵データの生成に用いた、相互認証鍵データを識別する相互認証コードを示す鍵指定データを生成する。

5 当該鍵指定データは、オーナーカード 72 またはユーザカード 73 の使用者が取得した、SAM ユニット 9 a, 9 b に係わる処理の実行権限を示すデータとなる。

ステップ S T 15 :

管理装置 20 のカード管理機能部 58 が、ステップ S T 13 で生成した縮退鍵データと、ステップ S T 14 で生成した鍵指定データとを、オーナーカード 72 またはユーザカード 73 の I C に書き込む。

10 ステップ S T 16 :

管理装置 20 のカード管理機能部 58 が、ステップ S T 13 の縮退鍵データの生成に用いた、相互認証鍵データを SAM ユニット 9 a, 9 b に登録する。

以下、上述した図 12 に示すステップ S T 12 で選択する対象となる相互認証鍵データについて説明する。

15 図 13 は、図 12 に示すステップ S T 12 で選択する対象となる相互認証鍵データを説明するための図である。

図 13 に示すように、当該相互認証鍵データには、例えば、デバイス鍵データ、ターミネーション鍵データ、製造設定サービス相互認証鍵データ、機器管理サービス相互認証鍵データ、通信管理サービス相互認証鍵データ、相互認証サービス相互認証鍵データ、A P 記憶領域管理サービス相互認証鍵データ、サービス A P 記憶領域相互認証鍵データ、システム A P 記憶領域相互認証鍵データ、並びに製造者 A P 記憶領域相互認証鍵データがある。

また、図 13 および図 14 に示すように、相互認証鍵データの相互認証コードが、図 14 に示すように、図 10 を用いて説明した A P 記憶領域 I D、エレメントタイプ番号、エレメントインスタンス番号およびエレメントバージョン番号から構成される。

以下、上述した図 1 2 に示すステップ S T 1 4 で生成する鍵指定データについて説明する。

当該鍵指定データは、上述した複数の相互認証鍵データの相互認証コードを用いて構成される、相互認証コードリストである。

5 図 1 5 は、鍵指定データの一例を説明するための図である。

図 1 2 のステップ S T 1 2 で、例えば、図 1 3 に示すデバイス鍵データ、機器管理サービス相互認証鍵データ、通信管理サービス相互認証鍵データ、A P 記憶領域管理サービス相互認証鍵データ、サービス A P 記憶領域相互認証鍵データ、並びにターミネーション鍵データが選択された場合には、図 1 5 (A) に示すよ

10 うに、当該選択された全ての相互認証鍵データの相互認証コードを示す鍵指定データが生成される。

図 1 2 に示すステップ S T 1 3 において、図 1 5 (A) に示す相互認証コードの相互認証鍵データを用いて縮退鍵データが生成された場合には、当該縮退鍵データを用いた S A M ユニット 9 a, 9 b との相互認証により、管理装置 2 0 に対して、図 1 5 (B) に示すように、機器管理サービス、通信管理サービス、I C サービス (I C カード 3 および I C モジュール 4 2 1 に関するサービス)、相互認証サービスおよび A P 記憶領域管理サービスが許可される。

15 このように、本実施形態では、S A M ユニット 9 a, 9 b の機能と、S A M ユニット 9 a, 9 b が保持するデータ (例えば、アプリケーションエレメントデータ A P E) へのアクセスを含む複数の処理にそれぞれ関連付けられた相互認証鍵データを用いて縮退鍵データを生成できる。

これにより、単数の縮退鍵データを用いた相互認証により、S A M ユニット 9 a, 9 b が、S A M ユニット 9 a, 9 b の機能と、S A M ユニット 9 a, 9 b が保持するデータへのアクセスとの双方について、それらを被認証手段に対して許可するか否かを一括して判断できる。

25 そして、S A M ユニット 9 a, 9 b は、被認証手段が正当であると認証した場

合に、当該被認証手段の指示に応じて、上記相互認証鍵データに関連付けられた所定の機能に係わる処理を実行すると共に、SAMユニット9a, 9bが保持するデータへの上記被認証手段からのアクセスを許可する。

以下、図12に示すステップST13の縮退処理方法について説明する。

5 図16は、当該縮退処理方法を説明するためのフローチャートである。

ステップST21：

管理装置20のカード管理機能部58が、デバイス鍵データをメッセージとし、
図12に示すステップST12で選択されたデバイス鍵データおよびターミネー
ション鍵データ以外の相互認証鍵データのうち最初の一つを暗号鍵として用いて、
10 デバイス鍵データを暗号化し、中間鍵データを生成する。

ここで、ステップST12で選択されたデバイス鍵データおよびターミネー
ション鍵データ以外の相互認証鍵データが一つの場合には、カード管理機能部58
は、上記中間鍵データを用いて次のステップST22の処理を行う。

一方、ステップST12で選択されたデバイス鍵データおよびターミネーショ
ン鍵データ以外の相互認証鍵データが2以上の場合には、カード管理機能部58
15 は、上記中間鍵データをメッセージとして、次の相互認証鍵データを暗号鍵とし
て用いて暗号化を行う。

カード管理機能部58は、ステップST12で選択されたデバイス鍵データお
よびターミネーション鍵データ以外の全ての相互認証鍵データを暗号鍵として用
20 いて上記暗号化を行うまで上記処理を繰り返し、終了したらステップST22の
処理に進む。

ステップST22：

カード管理機能部58が、ステップST21で得られた中間鍵データをメッセ
ージとして、ターミネーション鍵データを暗号鍵として用いて暗号化を行って縮
25 退鍵データを生成する。

当該ターミネーション鍵データは、改竄防止鍵データであり、管理者のみが保持

している。

これにより、管理者以外の者が、不正に縮退鍵データを改竄することを防止できる。

以下、上述したターミネーション鍵データとして、管理者（オーナー）のみが所有するオーナーターミネーション鍵データと、上記管理者から権限を与えられたユーザが所有するユーザターミネーション鍵データとを用いて、所定の縮退処理方法で、縮退鍵データを生成する場合を説明する。

図17は、当該縮退処理方法を説明するためのフローチャートである。

図17において、ステップST31、ST32の処理は、ターミネーション鍵データとして、上記オーナーターミネーション鍵データを用いる点を除いて、図16を用いて説明したステップST21、ST22の処理と同じである。

ステップST32で生成された縮退鍵データは、ユーザターミネーション鍵データを与えられたユーザが、拡張できるという意味で拡張可能な縮退鍵データである。

15 ステップST33：

管理装置20のカード管理機能部58が、オーナーが生成した拡張可能縮退鍵データをメッセージとし、ユーザが選択したユーザターミネーション鍵データ以外の相互認証鍵データのうち最初の一つを暗号鍵として用いて、デバイス鍵データを暗号化し、中間鍵データを生成する。

20 ここで、上記選択されたユーザターミネーション鍵データ以外の相互認証鍵データが一つの場合には、カード管理機能部58は、上記中間鍵データを用いて次のステップST22の処理を行う。

一方、上記選択されたユーザターミネーション鍵データ以外の相互認証鍵データが2以上の場合には、カード管理機能部58は、上記中間鍵データをメッセージとして、次の相互認証鍵データを暗号鍵として用いて暗号化を行う。

25 カード管理機能部58は、上記選択されたユーザターミネーション鍵データ以

外の全ての相互認証鍵データを暗号鍵として用いて上記暗号化を行うまで上記処理を繰り返し、終了したらステップS T 3 4の処理に進む。

ステップS T 3 4 :

5 カード管理機能部58が、ステップS T 3 3で得られた中間鍵データをメッセージとして、ユーザーミネーション鍵データを暗号鍵として用いて暗号化を行って縮退鍵データを生成する。

当該ユーザーミネーション鍵データは、改竄防止鍵データであり、上記オーナーおよび上記ユーザのみが保持している。

10 これにより、上記オーナーおよび上記ユーザ以外の者が、不正に縮退鍵データを改竄することを防止できる。

図17に示す処理によって生成された縮退鍵データは、図18に示すような階層で相互認証鍵が暗号化されたものになる。

また、本実施形態では、単数の相互認証鍵データ（例えば、図13に示すサービス、システム、製造者AP記憶領域相互認証鍵データ）に、複数のアプリケーション
15 ションエレメントデータAPEを関連付けてもよい。

これにより、縮退鍵データを用いた認証により、SAMユニット9a, 9bが、単数の相互認証鍵データに関連付けられたアプリケーションエレメントデータAPEへのアクセスを許可するか否かを一括して判断できる。

例えば、図19では、相互認証鍵データ500に、アプリケーションエレメントデータAPEのインスタンスaのパーミッションCと、インスタンスbのパー
20 ミッションBとが関連付けられている。そのため、相互認証鍵データ500を縮退した縮退鍵データを用いた認証が成功すれば、SAMユニット9a, 9bがインスタンスa, bの双方へのアクセスを許可する。

また、本実施形態では、図13を用いた説明した相互認証鍵データの全てある
25 一部について、図20に示すように、オンライン相互認証鍵データMK1とオフライン相互認証鍵データMK2とをペアで用いるようにしてもよい。

この場合には、相互認証を行う場合にはオンライン相互認証鍵データMK 1を用い、相互認証を行った相手とはデータ授受を行う場合には、それに対応するオフライン相互認証鍵データMK 2を用いて授受するデータを暗号化する。

5 これにより、仮にオンライン相互認証鍵データMK 1が不正に他人に取得された場合でも、被認証手段と認証手段とで授受するデータはオフライン相互認証鍵データMK 2で暗号化されているため、その情報が不正に漏れることを防止できる。

10 以下、例えば、図3に示すステップST 3などで行われる管理装置20のSAM管理機能部57とSAMユニット9a、9bとの間の相互認証について説明する。

この場合に、管理装置20が被認証手段となり、SAMユニット9a、9bが認証手段となる。

図2.1および図2.2は、管理装置20のSAM管理機能部57とSAMユニット9aとの間の相互認証について説明するためのフローチャートである。

15 SAMユニット9bについても、以下に示すSAMユニット9aの場合と同じである。

ステップST 51:

まず、管理者またはユーザが、オーナカード72またはユーザカード73を、カードリーダー・ライタ53にセットする。

20 そして、オーナカード72およびユーザカード73に記憶された縮退鍵データKa（本発明の第1の認証用データ）および鍵指定データが、管理装置20のSAM管理機能部57に読み込まれる。

SAM管理機能部57が、乱数Raを発生する。

ステップST 52:

25 SAM管理機能部57が、ステップST 51で読み込んだ縮退鍵データKaを用いて、ステップST 51で生成した乱数Raを、暗号化アルゴリズム1で暗号

化してデータR a' を生成する。

ステップS T 5 3 :

SAM管理機能部57が、ステップS T 5 1で読み込んだ鍵指定データと、ステップS T 5 2で生成したデータR a' とをSAMユニット9 aに出力する。

- 5 SAMユニット9 aは、図8に示す外部I/F62を介して、当該鍵指定データおよびデータR a' を入力して、これをメモリ63に格納する。

ステップS T 5 4 :

SAMユニット9 aの認証部64が、メモリ63あるいは外部メモリ7に記憶された相互認証鍵データのなかから、ステップS T 5 3で入力した鍵指定データ
10 が示す相互認証鍵データを特定する。

ステップS T 5 5 :

SAMユニット9 aの認証部64が、ステップS T 5 4で特定した相互認証鍵データを用いて、図16あるいは図17を用いて前述した縮退処理を行って縮退鍵データK bを生成する。

- 15 ステップS T 5 6 :

SAMユニット9 aの認証部64が、ステップS T 5 5で生成した縮退鍵データK bを用いて、上記暗号化アルゴリズム1に対応した復号アルゴリズム1で、ステップS T 5 3で入力したデータR a' を復号して乱数R aを生成する。

ステップS T 5 7 :

- 20 SAMユニット9 aの認証部64が、上記縮退鍵データK bを用いて、暗号化アルゴリズム2で、ステップS T 5 6で生成した乱数R aを暗号化して、データR a'' を生成する。

ステップS T 5 8 :

SAMユニット9 aの認証部64が、乱数R bを生成する。

- 25 ステップS T 5 9 :

SAMユニット9 aの認証部64が、上記縮退鍵データK bを用いて、ステッ

ステップST58で生成した乱数Rbを、暗号化アルゴリズム2で暗号化してデータRb'を生成する。

ステップST60:

SAMユニット9aの認証部64が、ステップST57で生成したデータRa''と、ステップST59で生成したデータRb'とを管理装置20に出力する。

ステップST61:

管理装置20のSAM管理機能部57が、縮退鍵データKaを用いて、上記暗号化アルゴリズム2に対応した復号アルゴリズム2で、ステップST60で入力したデータRa''およびRb'を復号してデータRa, Rbを生成する。

10 ステップST62:

管理装置20のSAM管理機能部57が、ステップST51で生成した乱数Raと、ステップST61で生成したデータRaとを比較する。

そして、SAM管理機能部57が、上記比較と結果が同じであることを示す場合に、SAMユニット9aが保持する上記縮退鍵データKbが、SAM管理機能部57が保持する上記縮退鍵データKaと同じであり、SAMユニット9aが正
15 当な認証手段であると認証する。

ステップST63:

管理装置20のSAM管理機能部57が、縮退鍵データKaを用いて、暗号化アルゴリズム1で、ステップST61で生成したデータRbを暗号化して、データRb''を生成する。
20

ステップST64:

管理装置20のSAM管理機能部57が、ステップST63で生成したデータRb''をSAMユニット9aに出力する。

ステップST65:

25 SAMユニット9aの認証部64が、縮退鍵データKbを用いて、ステップST64で入力したデータRb''を、復号アルゴリズム1で復号してデータRbを

生成する。

ステップST 6 6 :

SAMユニット9 aの認証部6 4が、ステップST 5 8で生成した乱数R bと、ステップST 6 5で生成したデータR bとを比較する。

- 5 そして、認証部6 4が、上記比較と結果が同じであることを示す場合に、SAMユニット9 aが保持する上記縮退鍵データK bが、SAM管理機能部5 7が保持する上記縮退鍵データK aと同じであり、SAM管理機能部5 7が正当な被認証手段であると認証する。

- 10 以下、図2 1および図2 2を用いて説明した相互認証の結果を基に、SAMユニット9 a, 9 bが行う処理を説明する。

図2 3は、SAMユニット9 a; 9 bの処理を説明するための図である。

ステップST 7 1 :

- 15 図8に示すSAMユニット9 a, 9 bのCPU 6 5が、図2 2に示すステップST 6 6において、認証部6 4が認証手段が正当であると認証したか否かを判断し、正当であると認証したと判断した場合にはステップST 7 2の処理に進み、そうでない場合には処理を終了する（すなわち、処理に係わる権限を有しないと判断し、処理を実行しない）。

ステップST 7 2 :

- 20 SAMユニット9 a, 9 bのCPU 6 5が、図2 1に示すステップST 5 4で特定した相互認証鍵データに関連付けられた処理を実行する。これによって、被認証手段が要求する所定のサービスが提供される。すなわち、SAMユニット9 a, 9 bが、被認証手段が所定の権限を有すると判断し、当該権限について許可した処理を実行する。

- 25 以下、図2および図4を用いて説明した管理装置2 0に関する各種のカードの発行に用いられる画面を説明する。

管理者等が、図2に示す操作部5 6を操作して、管理ツール5 2の操作画面表

示を指示すると、例えば、図24に示すように、SAM管理画面750がディスプレイ54に表示される。

SAM管理画面750には、ツールバーに管理ツール用カードの作成指示用の画像751が表示されている。

- 5 また、SAM管理画面750には、SAMネットワークに接続されたSAMのネットワーク構成を示す画像752が表示されている。

ユーザが、SAM管理画面750上で画像751を例えば操作部56のマウスなどで指定すると、画像753が表示される。

- 10 画像753には、オーナカードの作成、ユーザカードの作成、AP暗号化カードの作成、トランスポートカードの作成を指示する画像が表示される。

以下、画像751に示される各カードの作成を指示した場合の画面を説明する。

先ず、オーナカード作成の画面を説明する。

- 15 図24に示す画像751上のオーナカードの作成を上記マウスで管理者が指示すると、図2に示すカード管理機能部58が、図25に示すオーナカード作成画面760をディスプレイ54に表示する。

オーナカード作成画面760には、利用サービス選択画像761、サービスAP記憶領域指定画像762、システムAP領域指定画像763、デバイス/ターミネーション鍵指定画像764、並びに指定確定指示画像765が表示される。

- 20 利用サービス選択画像761は、例えば、作成するオーナカード72に許可するサービスの内容を選択するための画像である。

サービスAP記憶領域指定画像762は、作成するオーナカード72を用いたサービスAP記憶領域へのアクセスに対して許可する形態を選択するための画像である。

- 25 システムAP記憶領域指定画像763は、作成するオーナカード72を用いたシステムAP記憶領域へのアクセスに対して許可する形態を選択するための画像である。

デバイス／ターミネーション鍵指定画像764は、オーナカード72の作成に用いるデバイス鍵データおよびターミネーション鍵データを指定する画像である。

指定確定指示画像765は、上記指定した内容を確定させる指示を入力するための画像である。

- 5 管理者は、オーナカード作成画面760上で必要な項目の指定を完了すると、上記マウスなどで指定確定指示画像765を指定する。

これにより、図26に示すカードセット指示画面770がディスプレイ54に表示される。

- 10 オーナカード72の作成時には、カードセット指示画面770は、デフォルトカード71をセットする旨を指示する。

そして、管理者は、デフォルトカード71のICのデータをカードリーダー・ライタ53に読み取らせる。

- 15 SAM管理機能部57は、デフォルトカード71の正当性を確認すると、オーナカード作成画面760上で管理者が選択したサービス等に関連付けられた相互認証鍵データを選択する。当該選択が、図12を用いて説明したステップST12の選択に対応する。

次に、ユーザカード作成の画面を説明する。

- 20 図24に示す画像751上のユーザカードの作成を上記マウスで管理者が指示すると、図2に示すカード管理機能部58が、図27に示すユーザカード作成画面780をディスプレイ54に表示する。

ユーザカード作成画面780には、利用サービス選択画像781、サービスAP記憶領域指定画像782、システムAP領域指定画像783、デバイス／ターミネーション鍵指定画像784、並びに指定確定指示画像785が表示される。

- 25 利用サービス選択画像781は、例えば、作成するユーザカード73に許可するサービスの内容を選択するための画像である。

サービスAP記憶領域指定画像782は、作成するユーザカード73を用いた

サービスAP記憶領域へのアクセスに対して許可する形態を選択するための画像である。

システムAP記憶領域指定画像783は、作成するユーザカード73を用いたシステムAP記憶領域へのアクセスに対して許可する形態を選択するための画像

5 である。

デバイス/ターミネーション鍵指定画像784は、ユーザカード73の作成に用いるデバイス鍵データおよびターミネーション鍵データを指定する画像である。

指定確定指示画像785は、上記指定した内容を確定させる指示を入力するための画像である。

10 管理者は、オーナカード作成画面780上で必要な項目の指定を完了すると、上記マウスなどで指定確定指示画像785を指定する。

これにより、図26に示すカードセット指示画面770がディスプレイ54に表示される。

15 ユーザカード73の作成時には、カードセット指示画面770は、オーナカード72をセットする旨を指示する。

そして、管理者は、オーナカード72のICのデータをカードリーダー・ライター53に読み取らせる。

SAM管理機能部57は、オーナカード72の正当性を確認すると、ユーザカード作成画面780上で管理者が選択したサービス等に関連付けられた相互認証
20 鍵データを選択する。当該選択が、図12を用いて説明したステップST12の選択に対応する。

次に、AP暗号化カード作成の画面を説明する。

図24に示す画像751上のAP暗号化カードの作成を上記マウスで管理者が指示すると、図2に示すカード管理機能部58が、図28に示すAP暗号化カー

25 ド作成画面790をディスプレイ54に表示する。

AP暗号化カード作成画面790には、利用サービス選択画像791、サービ

スAP記憶領域指定画像792、システムAP領域指定画像793、デバイス／ターミネーション鍵指定画像794、並びに指定確定指示画像795が表示される。

5 利用サービス選択画像791は、例えば、作成するAP暗号化カード75に許可するサービスの内容を選択するための画像である。

サービスAP記憶領域指定画像792は、作成するAP暗号化カード75を用いたサービスAP記憶領域へのアクセスに対して許可する形態を選択するための画像である。

10 システムAP記憶領域指定画像793は、作成するAP暗号化カード75を用いたシステムAP記憶領域へのアクセスに対して許可する形態を選択するための画像である。

デバイス／ターミネーション鍵指定画像794は、AP暗号化カード75の作成に用いるデバイス鍵データおよびターミネーション鍵データを指定する画像である。

15 指定確定指示画像795は、上記指定した内容を確定させる指示を入力するための画像である。

管理者は、AP暗号化カード作成画面790上で必要な項目の指定を完了すると、上記マウスなどで指定確定指示画像795を指定する。

20 これにより、図26に示すカードセット指示画面770がディスプレイ54に表示される。

AP暗号化カード75の作成時には、カードセット指示画面770は、例えば、オーナカード72をセットする旨を指示する。

そして、管理者は、オーナカード72のICのデータをカードリーダー・ライター53に読み取らせる。

25 SAM管理機能部57は、オーナカード72の正当性を確認すると、AP暗号化カード作成画面790上で管理者が選択したサービス等に関連付けられた相互

認証鍵データを選択する。当該選択が、図12を用いて説明したステップST12の選択に対応する。

次に、トランスポートカード作成の画面を説明する。

図24に示す画像751上のトランスポートカードの作成を上記マウスで管理者が指示すると、図2に示すカード管理機能部58が、図29に示すトランスポートカード作成画面800をディスプレイ54に表示する。

トランスポートカード作成画面800は、データの搬送の対象として許可するSAMのIPアドレス、AP記憶領域、アプリケーションエレメントデータAPEのAPEタイプ、インスタンス番号およびバージョンを指定する画像を表示する。

カード管理機能部58は、トランスポートカード作成画面800上で指定された情報を基に、SAMユニット9a、9bの記憶領域内のアクセスが許可されたデータに関連付けられた相互認証鍵データを縮退して縮退鍵データを生成し、これをトランスポートカード74に書き込む。

上述したように、SAMユニット9a、9bが提供する処理等を機能的に示した画面を基に、その機能を管理者等が、選択して各種のカードを発行することで、当該処理に実際に用いられる相互認証鍵データなどを、管理者に具体的に明示することなく、管理者が自らの意向に合った権限を持つカードを発行できる。これにより、SAMユニット9a、9bのセキュリティに係わる情報が漏れることを回避できる。

以下、図2に示す管理ツール52のSAM管理機能部57が提供するSAM管理画面を説明する。

図30は、SAM管理画面1001を説明するための図である。

管理者等が、図2に示す操作部56を操作して、管理ツール52にSAM管理画面表示指示を認証要求先すると、例えば、図30に示すSAM管理画面1001がディスプレイ54に表示される。

図30に示すように、SAM管理画面1001は、メニュー・バー1002、SAMツリー領域1003、属性情報表示領域1004、詳細情報表示領域1005およびコンソール領域1006を有する。

メニュー・バー1002は、図2に示すカード管理機能部58の各種操作を指定するために用いられる。

当該操作には、ファイル操作、SAMコマンド操作、管理ツール用カード操作、コンソールログ操作およびヘルプ操作などがある。

SAMツリー領域1003には、SAM管理機能部57で操作するSAM（SAMユニット9a，9b）と、そのSAMが属するグループが表示される。

10 ユーザは、SAMツリー領域1003上で、操作対象となるSAMを選択する。

属性情報表示領域1004には、SAMツリー領域1003で選択したSAMやグループの情報が表示される。

15 詳細情報表示領域1005には、SAMツリー領域1003で選択したSAMやグループ内の各種情報の一覧が表示される。

コンソール領域1006には、SAMに対する各種操作の情報および結果が表示される。

図31は、SAMツリー領域1003の表示内容の一例を示す画面を説明するための図である。

20 図31に示すように、SAMツリー領域1003には、SAM管理機能部57で操作するSAMと、そのSAMが属するグループ等を示す種々のアイコンが表示される。

図32は、SAMツリー領域1003に表示されるアイコンを説明するための図である。

25 図32に示すように、SAMツリー領域1003に表示されるアイコンには、物体やデータを示すものとして、SAMネットワーク、グループ（SAMの集合

体)、SAM (1台のSAM)、AP記憶領域、APEタイプ、インスタンスのアイコンがある。

また、SAMの状態を示すアイコンとして、SAMがサービスが開始されていない状態であることを示す「STANBY」、SAMが通常状態であることを示す「READY」、相互認証済の接続状態であることを示す「READY」、他の接続が完了するのを待っている状態であることを示す「SINGLE CONNECTION WAIT」、管理ツール52のみが接続していることを示す「SINGLE CONNECTION」などのアイコンがある。

10 このように、SAMツリー領域1003には、SAMに対応する画像を、SAMの動作状態に応じて異なる複数のパターンを用いて表示する。

これにより、ユーザは、SAMの状態を容易に特定できる。

また、SAMツリー領域1003には、SAMに対応する画像、当該SAMが相互認証済であるか、すなわち、被認証手段の正当性を既に認めたか否かを識別可能なパターンで表示するため、各SAMが相互認証を終えたか否かをユーザが
15 容易に特定できる。

図33は、SAMネットワーク画面1010を説明するための図である。

図31に示すSAMツリー領域1003上で、ユーザがマウス等でSAMネットワークのアイコンを指定すると、図33に示すSAMネットワーク画面1010がディスプレイ54に表示される。

20 SAMネットワーク画面1010には、SAMネットワークに接続されたSAMのIPアドレス、ポートおよび状態と、グループとについての情報が表示される。

図34は、グループ画面1020を説明するための図である。

図31に示すSAMツリー領域1003上で、ユーザがマウス等でグループの
25 アイコンを指定すると、図34に示すグループ画面1020がディスプレイ54に表示される。

グループ画面 1020 には、指定されたグループに属する SAM の IP アドレス、ポートおよび状態についての情報が表示される。

図 35 は、SAM 画面 1030 を説明するための図である。

- 5 図 31 に示す SAM ツリー領域 1003 上で、ユーザがマウス等で SAM のアイコンを指定すると、図 35 に示す SAM 画面 1030 がディスプレイ 54 に表示される。

SAM 画面 1030 には、指定された SAM の AP 記憶領域の ID、並びに、その AP 記憶領域の用途についての情報が表示される。

図 36 は、AP 記憶領域画面 1040 を説明するための図である。

- 10 図 31 に示す SAM ツリー領域 1003 上で、ユーザがマウス等で AP 記憶領域のアイコンを指定すると、図 36 に示す AP 記憶領域画面 1040 がディスプレイ 54 に表示される。

AP 記憶領域画面 1040 には、指定された AP 記憶領域の APE タイプの番号、APE タイプの種類についての情報が表示される。

- 15 図 37 は、APE タイプ画面 1050 を説明するための図である。

図 31 に示す SAM ツリー領域 1003 上で、ユーザがマウス等で APE タイプのアイコンを指定すると、図 37 に示す APE タイプ画面 1050 がディスプレイ 54 に表示される。

- 20 APE タイプ画面 1050 には、指定された APE タイプを用いて構成されるインスタンスの番号、システムコード、エリア/サービスコードなどについての情報が表示される。

図 38 は、インスタンス画面 1060 を説明するための図である。

- 25 図 31 に示す SAM ツリー領域 1003 上で、ユーザがマウス等でインスタンスのアイコンを指定すると、図 38 に示すインスタンス画面 1060 がディスプレイ 54 に表示される。

インスタンス画面 1060 には、指定されたインスタンスの動作状態、記憶領

域、ICサービス鍵およびインスタンス番号などの情報が表示される。

図39は、図30に示すメニュー・バー1002のSAMコマンドを指定した場合の画面である。

図30に示すメニュー・バー1002上で、ユーザがマウス等でSAMコマンドのアイコンを指定すると、図39に示すSAMコマンド画面1070がディスプレイ54に表示される。

SAMコマンド画面1070には、SAMについての操作である、通信管理、AP記憶領域管理、ログ記録、ネガリスト、製造設定などの文字画像が表示されている。

10 ここで、ユーザが、通信管理を指定すると、ステータス取得、サービス開始、アクティベーションコード変更、シングルコネクション開始、コネクション切断などの文字画像が表示される。

ユーザは、これらの文字画像を指定することで、SAMに対しての操作を行う。

図40は、図30に示すSAM管理画面1001上でSAMのグループを作成
15 する場合を説明するための図である。

図40に示すように、SAM管理画面1001上のSAMツリー領域1003のSAM管理の文字画像上で、ユーザがマウスなどで右クリックを行うと、操作画面1100が表示される。

操作画面1100には、SAMのグループ作成、SAMの追加およびSAMの
20 最新状態を取得するなどの指示を行うための文字画像が表示される。

ユーザは、例えば、SAMのグループ作成の文字画像をマウスなどで指定することで、選択した複数のSAMからなるグループを規定することができる。

その場合に、SAM管理機能部57から、グループに鍵指定データを出力する指示を出すだけで、当該グループに属する全てのSAM（SAMユニット9a，
25 9b）に対して、当該鍵指定データが一括して提供される。

また、SAM管理機能部57からの指示に応じて、当該グループに属する全て

のSAMに対して、SAM管理機能部57が保持する縮退鍵データに対応した相互認証データに関連付けられた処理を一括して行わせることができる。

以下、図2に示すAP編集ツール51が提供するAP記憶領域エディタについて説明する。

5 図41は、AP記憶領域エディタ画面1200を説明するための図である。

図41に示すように、AP記憶領域エディタ画面1200は、編集の対象とするAP記憶領域に格納されたアプリケーションエレメントデータAPEのAPEタイプおよびインスタンス番号を表示する。

10 また、AP記憶領域エディタ画面1200には、追加を示すアイコン1210、削除を示すアイコン1220、編集を示すアイコン1230が表示されている。

ユーザがマウスなどでアイコン1210を指定すると、当該AP記憶領域に対してのインスタンスの追加処理が行われる。

また、アイコン1210を指定すると、当該AP記憶領域に記憶されているインスタンスの削除処理が行われる。

15 また、アイコン1210を指定すると、当該AP記憶領域に記憶されているインスタンスの編集処理が行われる。

図42は、アプリケーションエレメントデータAPEのパッケージの追加を行うための画面1300を説明するための図である。

20 画面1300には、エレメントの作成、バージョンの追加の何れを行うかを指定する欄1301と、APEタイプを選択する欄1302と、インスタンス番号を指定する欄1303がある。

ユーザは、欄1301、1302および1303に追加するパッケージに関する情報を入力する。

25 これにより、AP編集ツール51が、自動的にエレメントパッケージの追加処理を行う。

図43は、アプリケーションエレメントデータAPEの作成を行うための画面

1400を説明するための図である。

図42に示す画面1300上で所定の情報を入力して、画像1304を指定すると、図43に示すAPE作成画面1400が表示される。

5 APE作成画面1400には、作成対象とするアプリケーションエレメントデータAPEのタイプ、そのインスタンスの番号が表示される。

また、APE作成画面1400には、タグを指定する欄1401、使用バージョン数を指定する欄1402、エレメント取得の可否を指定する欄1403、データ自動生成の可否を指定する欄1404、並びにエレメント削除を指定する欄1405が表示される。

10 また、作成対象のアプリケーションエレメントデータAPEに関連付けられる各種の相互認証鍵データなどの属性情報名や値などを指定する欄1406が表示される。

図44は、アプリケーションエレメントデータAPEのバージョン追加を行うための画面1500を説明するための図である。

15 図42に示す画面1300上で、欄1301でバージョン追加を指定し、所定の情報を入力して、画像1304を指定すると、図44に示すAPEバージョン追加画面1500が表示される。

APEバージョン追加画面1500には、作成対象とするアプリケーションエレメントデータAPEのタイプ、そのインスタンスの番号が表示される。

20 また、APEバージョン追加画面1500には、エレメントバージョンを指定する欄1501、鍵データ入力方法を指定する欄1502、並びにエレメントデータの項目名および値を指定する欄1503が表示される。

上述した図42～図44に示す画面を用いて、アプリケーションエレメントデータAPEの作成およびバージョン追加を行うと、図45に示すように、AP記憶領域エディタ画面1200には、作成および追加したアプリケーションエレメントデータAPEに関する情報が欄1240に表示される。

25

以上説明したように、管理装置 20 によれば、図 12 および図 16 等を用いて説明したように、SAM ユニット 9a, 9b に係わる処理に関連付けられた複数の相互認証鍵データを用いて縮退処理を行い、縮退鍵データを生成する。

そして、オーナーカード 72 やユーザカード 73 に、当該縮退鍵データ、並びに
5 その生成に用いた相互認証鍵データを特定するための鍵指定データを書き込む。

また、オーナーカード 72 等を用いた管理装置 20 と SAM ユニット 9a, 9b との間で、図 21 ~ 図 23 を用いた相互認証を行うことで、SAM ユニット 9a が管理装置 20 から受けた鍵指定データを基に縮退鍵データを生成し、当該縮退鍵データが管理装置 20 が保持するものと一致した場合に、被認証手段である管
10 理装置 20 の正当性を確認できる。

また、その確認と共に、鍵指定データによって指定された相互認証鍵データに関連付けられた処理を、管理装置 20 に許可された処理であると判断できる。

そのため、認証手段である SAM ユニット 9a, 9b は、従来のように全ての被認証手段（例えば、オーナーカード 72 およびユーザカード 73 を用いた管理装
15 置 20 等）に対応した相互認証鍵データを保持する必要がなく、しかも、被認証手段に許可した処理を管理テーブルで管理する必要もなく、処理負担が軽減される。

本発明は上述した実施形態には限定されない。

本発明は、例えば、オーナーカード 72、ユーザカード 73、トランスポートカード 74 および AP 暗号化カード 75 の何れかのカードの IC に、そのカードの
20 使用者の生体情報を記憶させ、SAM ユニット 9a, 9b が、上述した相互認証と共に、当該カードに記憶された生体情報をさらに用いて、その使用者の正当性を認証してもよい。

例えば、上述した実施形態では、SAM ユニット 9a, 9b が管理装置 20 と
25 相互認証を行う場合を例示したが、SAM ユニット 9a, 9b が ASP サーバ装置 19a, 19b や他の SAM ユニットなどの被認証手段と認証を行ってもよい。

この場合には、当該被認証手段が、上述した縮退鍵データおよび鍵指定データを保持する。

また、上述した実施形態では、オーナーカード 7 2 およびユーザカード 7 3 が、上述した縮退鍵データおよび鍵指定データを保持する場合を例示したが、その他
5 の携帯装置などに、これらのデータを保持させてもよい。

産業上の利用可能性

本発明は、認証結果を基に所定の処理を行うデータ処理方法、そのプログラム
およびその装置に適用可能である。

請 求 の 範 囲

1. 鍵データを用いて暗号化を行って生成された第1の認証用データを保持する被認証手段と、前記鍵データを保持する認証手段とが行うデータ処理方法で

5 あって、

前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手段に提供する第1の工程と、

前記認証手段が、前記第1の工程で受けた前記鍵指定データが指定する前記鍵データを用いて暗号化を行って第2の認証用データを生成する第2の工程

10 と、

前記被認証手段が前記第1の認証用データを用い、前記認証手段が前記第2の認証用データを用いて、認証を行う第3の工程と、

前記認証手段が、前記第3の工程の前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断すると、前記鍵データに

15 関連付けられた処理を実行する第4の工程と

を有するデータ処理方法。

2. 鍵データを用いて暗号化を行って生成された第1の認証用データを保持する被認証手段と、

前記鍵データを保持する認証手段と

20 を有し、

前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手段に提供し、

前記認証手段が、前記被認証手段から受けた前記鍵指定データが指定する前記鍵データを用いて前記暗号化を行って第2の認証用データを生成し、

25 前記被認証手段が前記第1の認証用データを用い、前記認証手段が前記第2の認証用データを用いて、認証を行い、

前記認証手段が、前記認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであると判断すると、前記鍵データに関連付けられた処理を実行する

データ処理システム。

- 5 3. 所定の鍵データを保持する認証手段が、前記鍵データを用いて暗号化を行って生成された第 1 の認証用データを保持する被認証手段と認証を行うデータ処理方法であって、

前記鍵データを指定する鍵指定データを前記被認証手段から受ける第 1 の工程と、

- 10 前記第 1 の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記暗号化を行って第 2 の認証用データを生成する第 2 の工程と、

前記第 2 の工程で生成した前記第 2 の認証用データを用いて、前記第 1 の認証用データを認証に用いる前記被認証手段と前記認証を行う第 3 の工程と、

- 15 前記第 3 の工程の前記認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処理を実行する第 4 の工程と

を有するデータ処理方法。

- 20 4. 前記第 4 の工程において、前記鍵データに関連付けられた、前記被認証手段に許可された前記認証手段の機能、または前記認証手段が保持するデータへのアクセスを実行する

請求項 3 に記載のデータ処理方法。

5. 前記認証用データが異なる複数の前記鍵データを用いて生成されている場合に、

- 25 前記第 4 の工程において、前記複数の鍵データにそれぞれ関連付けられた複数の処理を実行する

請求項 3 に記載のデータ処理方法。

6. 前記第4の工程において、前記複数の鍵データにそれぞれ関連付けられた、前記認証手段の機能および前記認証手段が保持するデータへのアクセスを含む複数の処理を実行する

請求項5に記載のデータ処理方法。

5 7. 前記第4の工程において、前記認証手段が複数のデータモジュールを前記データとして保持している場合に、単数の前記鍵データに関連付けられた、複数の前記データモジュールへのアクセスを実行する

請求項3に記載のデータ処理方法。

10 8. 前記第1の工程において、前記第1の認証用データおよび前記鍵指定データを保持する集積回路から前記被認証手段の装置が読み出した前記鍵指定データを受ける

請求項3に記載のデータ処理方法。

9. 前記第1の認証用データは、所定のデータを前記鍵データを用いて暗号化して生成されたデータである

15 請求項3に記載のデータ処理方法。

10. 前記第1の認証用データは、前記所定のデータを前記鍵データを用いて暗号化して得られたデータを、管理元が管理する改竄防止鍵データをさらに用いて暗号化して生成されたデータである

請求項9に記載のデータ処理方法。

20 11. 所定の鍵データを用いて暗号化を行って生成された第1の認証用データを保持する被認証手段と認証を行い、前記鍵データを保持するデータ処理装置であって、

前記被認証手段から、前記鍵データを指定する鍵指定データを入力する入力手段と、

25 前記入力手段が受けた前記鍵指定データが指定する前記鍵データを用いて暗号化を行って第2の認証用データを生成し、当該第2の認証用データを用い

て、前記第 1 の認証用データを認証に用いる前記被認証手段と前記認証を行う認証手段と、

前記認証手段が前記認証により前記第 1 の認証用データと前記第 2 の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処

5 理を実行する制御手段と

を有するデータ処理装置。

1. 2. 所定の鍵データを用いて暗号化を行って生成された第 1 の認証用データを保持する被認証手段と認証を行い、前記所定の鍵データを保持するデータ処理装置が実行するプログラムであって、

10 前記鍵データを指定する鍵指定データを前記被認証手段から受ける第 1 の手順と、

前記第 1 の手順で受けた前記鍵指定データが指定する前記鍵データを用いて前記暗号化を行って第 2 の認証用データを生成する第 2 の手順と、

15 前記第 2 の手順で生成した前記第 2 の認証用データを用いて、前記第 1 の認証用データを認証に用いる前記被認証手段と前記認証を行う第 3 の手順と、

前記第 3 の手順の前記認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処理を実行する第 4 の手順と

を有するプログラム。

20 1. 3. 鍵データを保持する認証手段が、第 1 の認証用データを保持する被認証手段から指定された前記鍵データを用いて暗号化を行って第 2 の認証用データを生成し、前記第 2 の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、
25 前記被認証手段が行うデータ処理方法であって、

前記所定の生成方法を基に前記第 1 の認証用データを生成したときに用

いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の工程と、

前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2 の工程と、

5 前記第 2 の工程の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第 3 の工程と

を有するデータ処理方法。

1 4. 前記被認証手段は、所定の集積回路から前記第 1 の認証用データおよび前記鍵指定データを読み出して保持する

10 請求項 1 3 に記載のデータ処理方法。

1 5. 前記第 3 の工程において、前記鍵データに関連付けられた、前記被認証手段に許可された前記認証手段の機能を前記認証手段に実行させるか、または、前記認証手段が保持するデータへのアクセスを実行する

請求項 1 3 に記載のデータ処理方法。

15 1 6. 複数の前記認証手段からなるグループを規定した場合に、前記第 1 の工程において、前記グループに対して前記鍵指定データを一括して提供し、

前記第 3 の工程において、前記グループに対して前記鍵データに関連付けられた処理を一括して行わせる

20 請求項 1 3 に記載のデータ処理方法。

1 7. 前記処理を行う前記認証手段に対応する画像を、前記認証手段の動作状態に応じて異なる複数のパターンを用いて表示する画面を提供する第 4 の工程

をさらに有する請求項 1 3 に記載のデータ処理方法。

1 8. 前記第 4 の工程において、前記第 2 の工程の認証により前記認証手段が、
25 前記被認証手段の正当性を既に認めたか否かを識別可能なパターンで、前記認証手段に対応する画像を表示した前記画面を提供する

請求項 17 に記載のデータ処理方法。

19. 鍵データを保持する認証手段が、第 1 の認証用データを保持する被認証手段から指定された前記鍵データを用いて暗号化を行って第 2 の認証用データを生成し、前記第 2 の認証用データを用いて前記被認証手段と認証を行い、当該認
5 証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、前記被認証手段を構成するデータ処理装置であって、

前記所定の生成方法を基に前記第 1 の認証用データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の手段
10 と、

前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2 の手段と、

前記第 2 の手段の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第 3 の手段と

15 を有するデータ処理装置。

20. 鍵データを保持する認証手段が、第 1 の認証用データを保持する被認証手段から指定された前記鍵データを用いて暗号化を行って第 2 の認証用データを生成し、前記第 2 の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、
20 前記被認証手段を構成するデータ処理装置によって実行されるプログラムであって、

前記所定の生成方法を基に前記第 1 の認証用データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の手順
25 と、

前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2

の手順と、

前記第 2 の手順の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第 3 の手順と
を有するプログラム。

FIG. 1

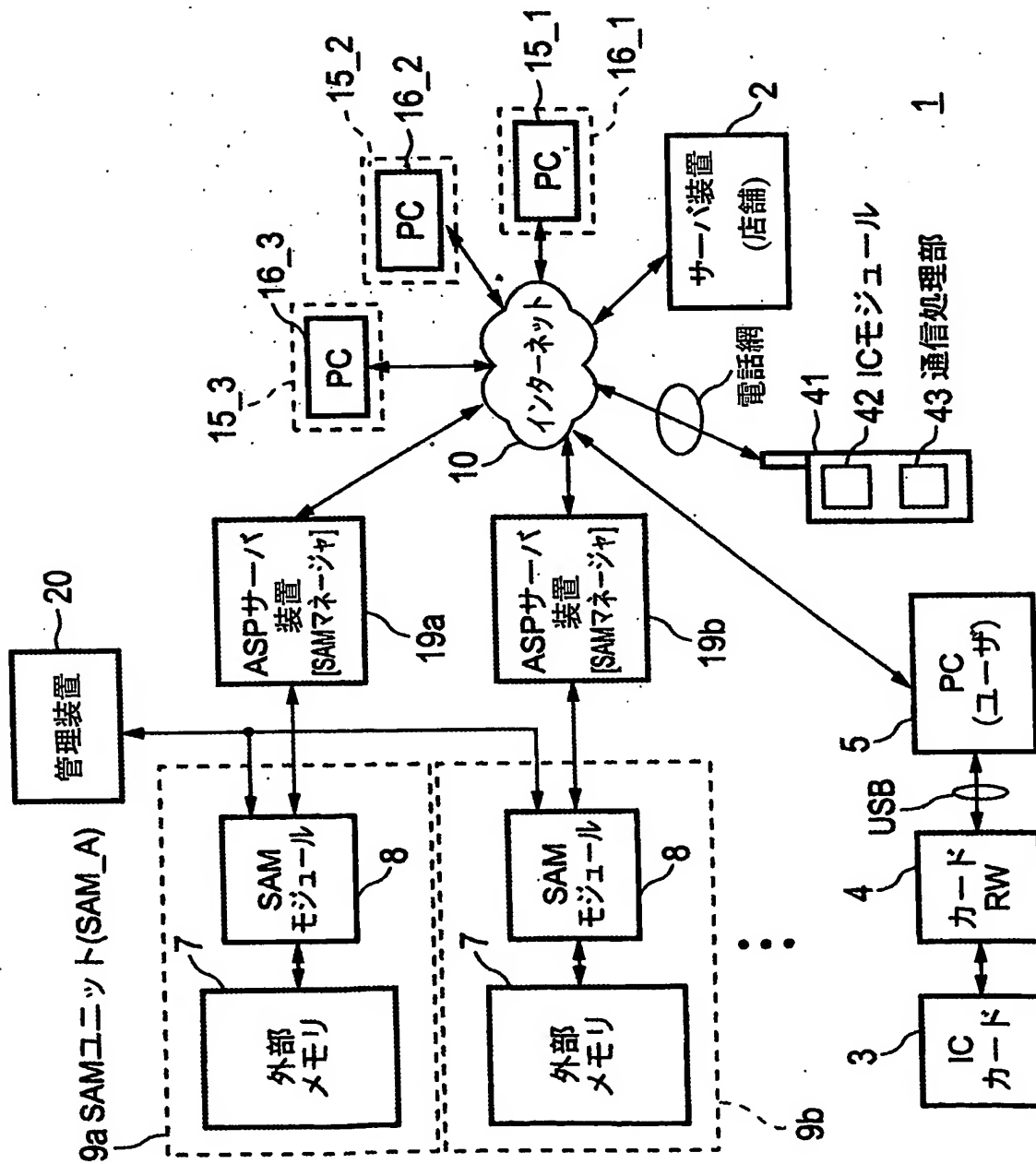


FIG. 2

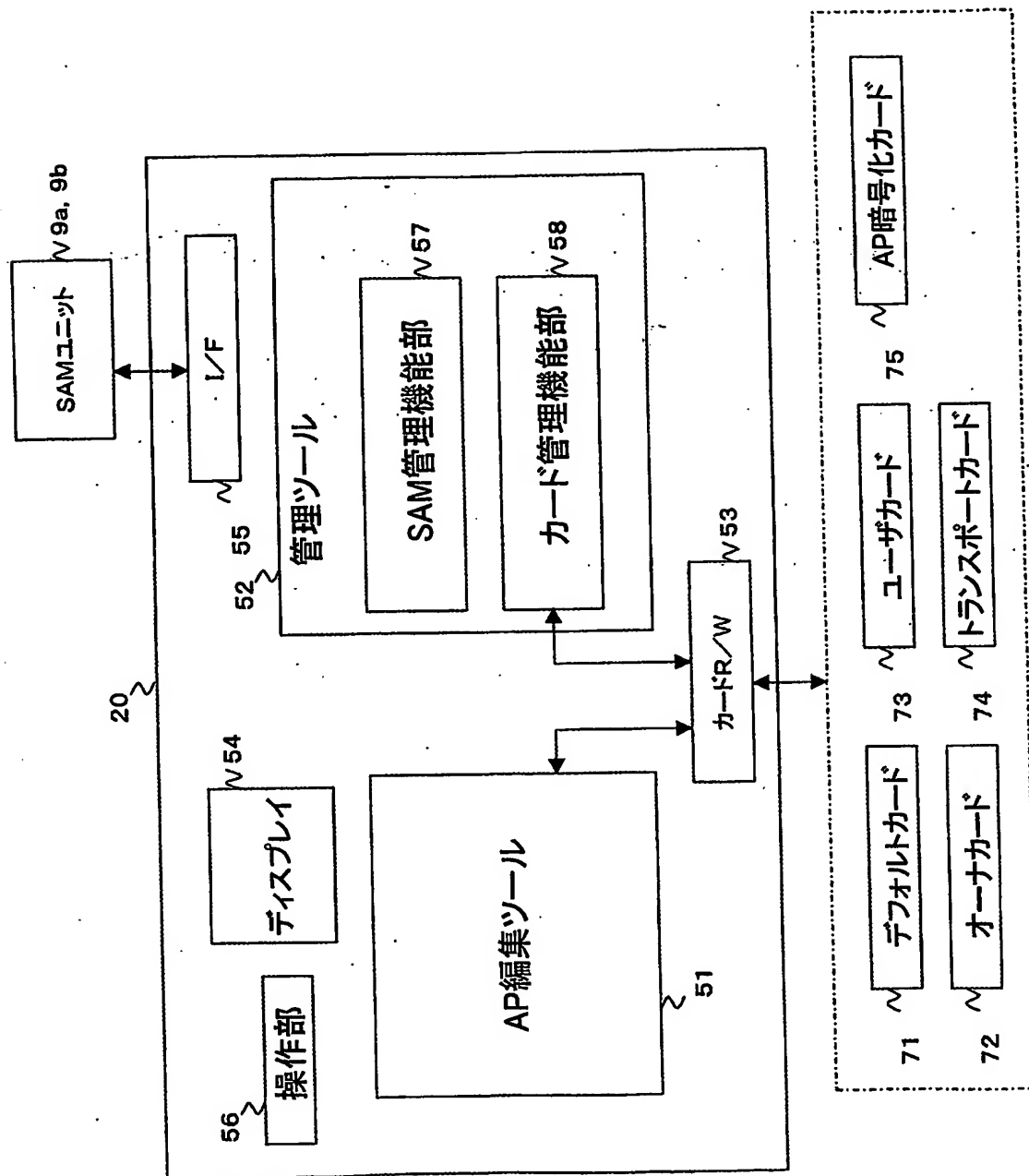


FIG. 3

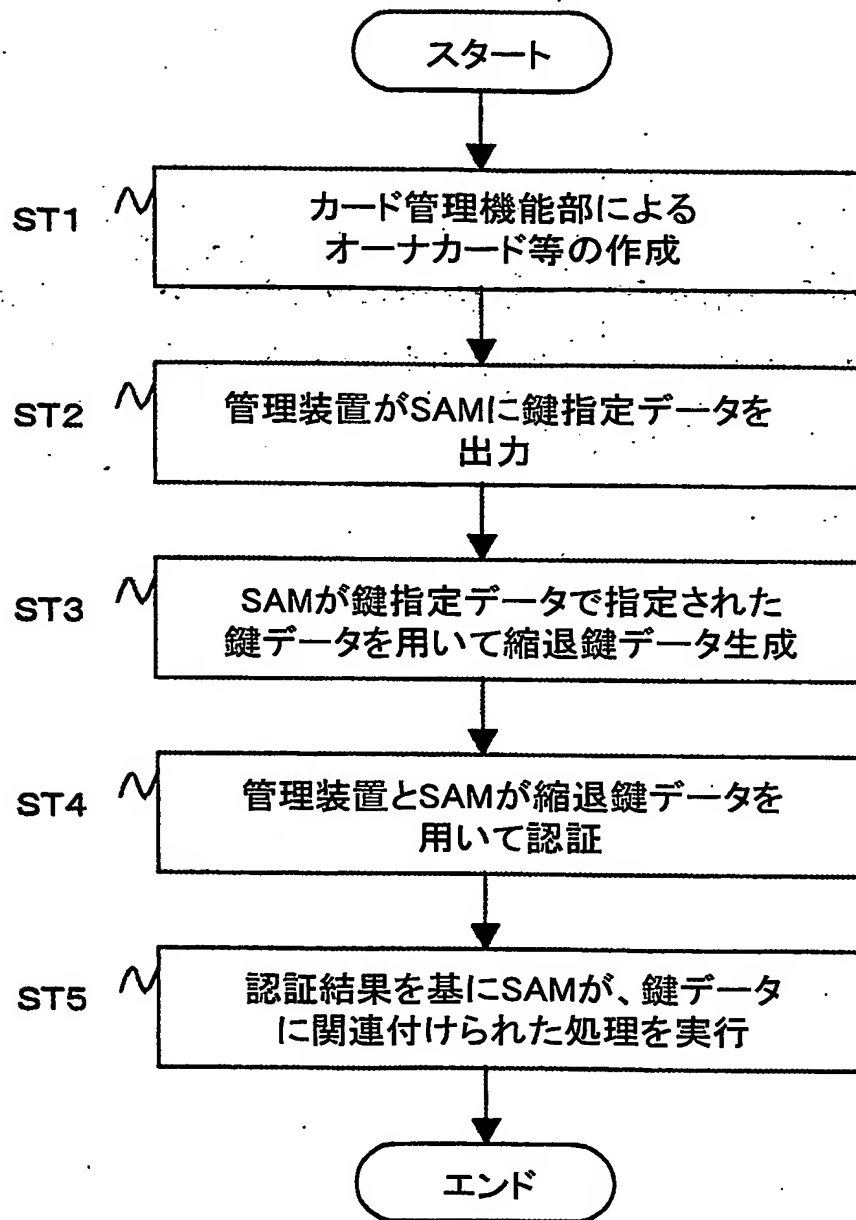


FIG. 4

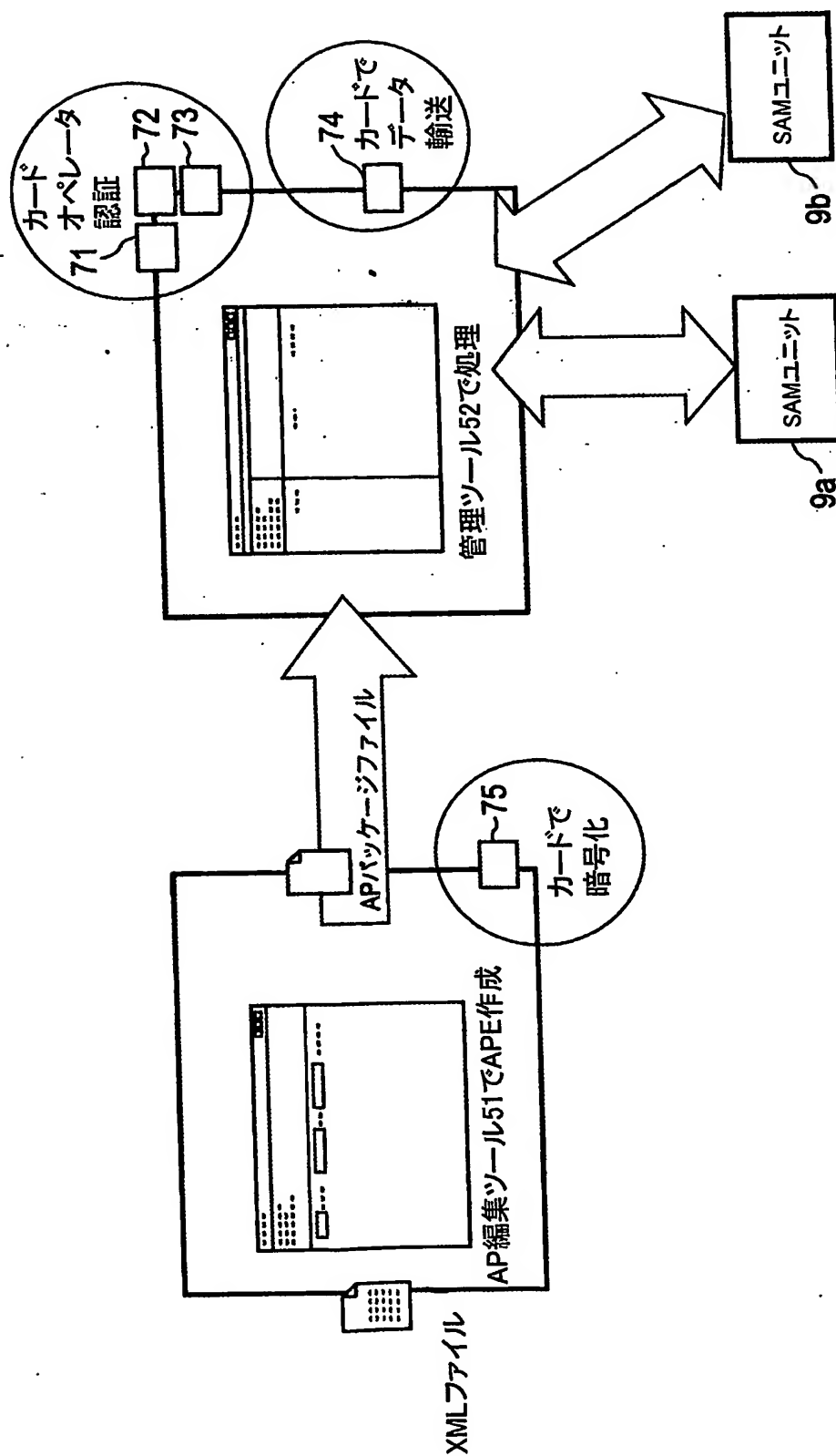


FIG. 5

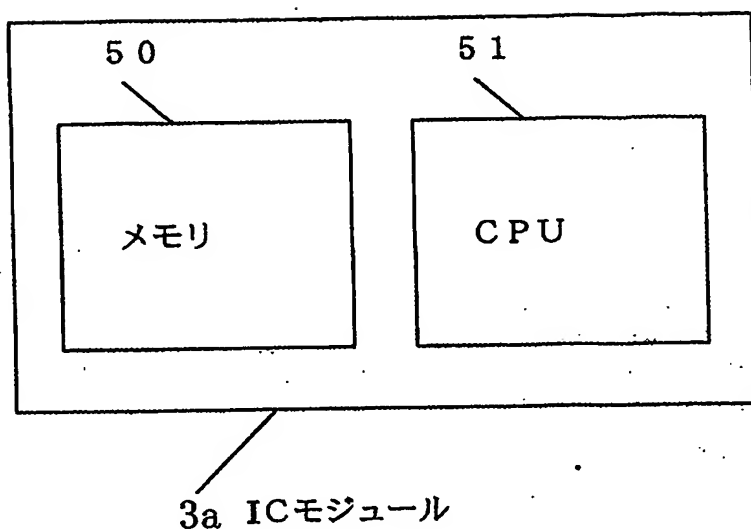


FIG. 6

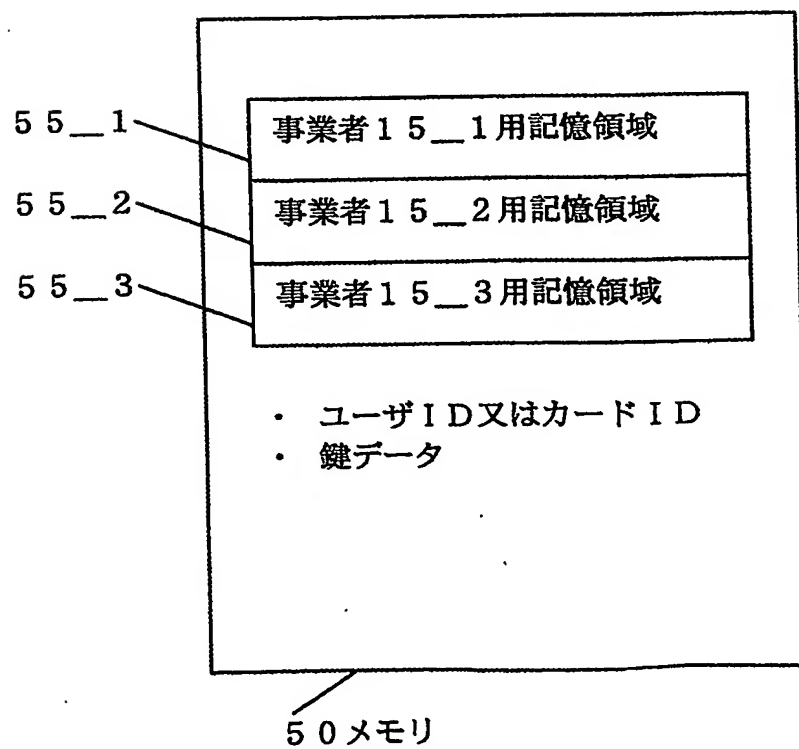


FIG. 7

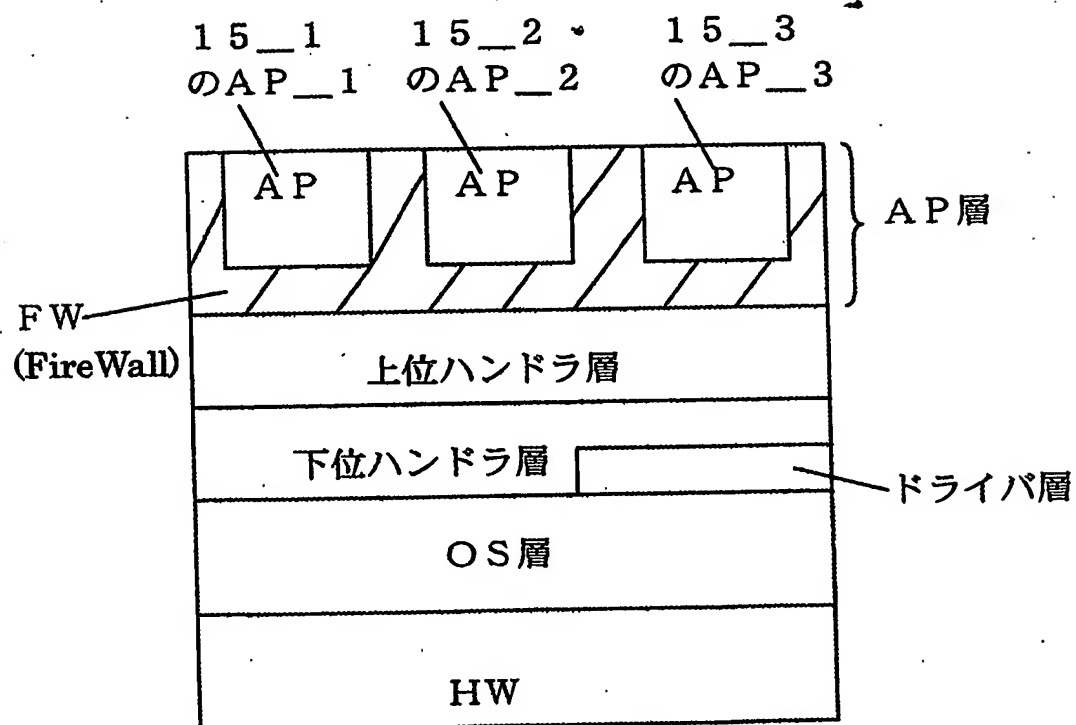


FIG. 8

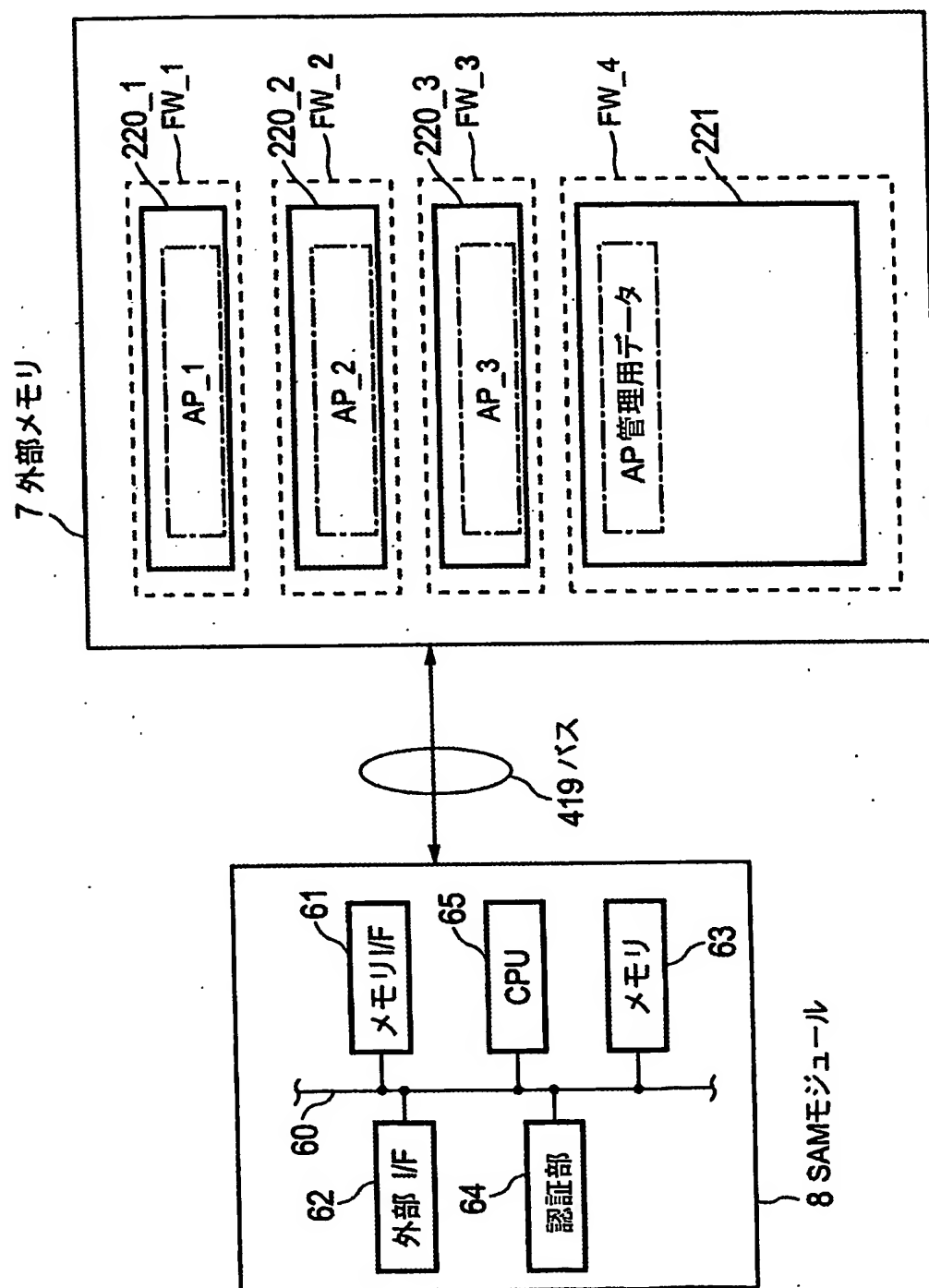


FIG. 9

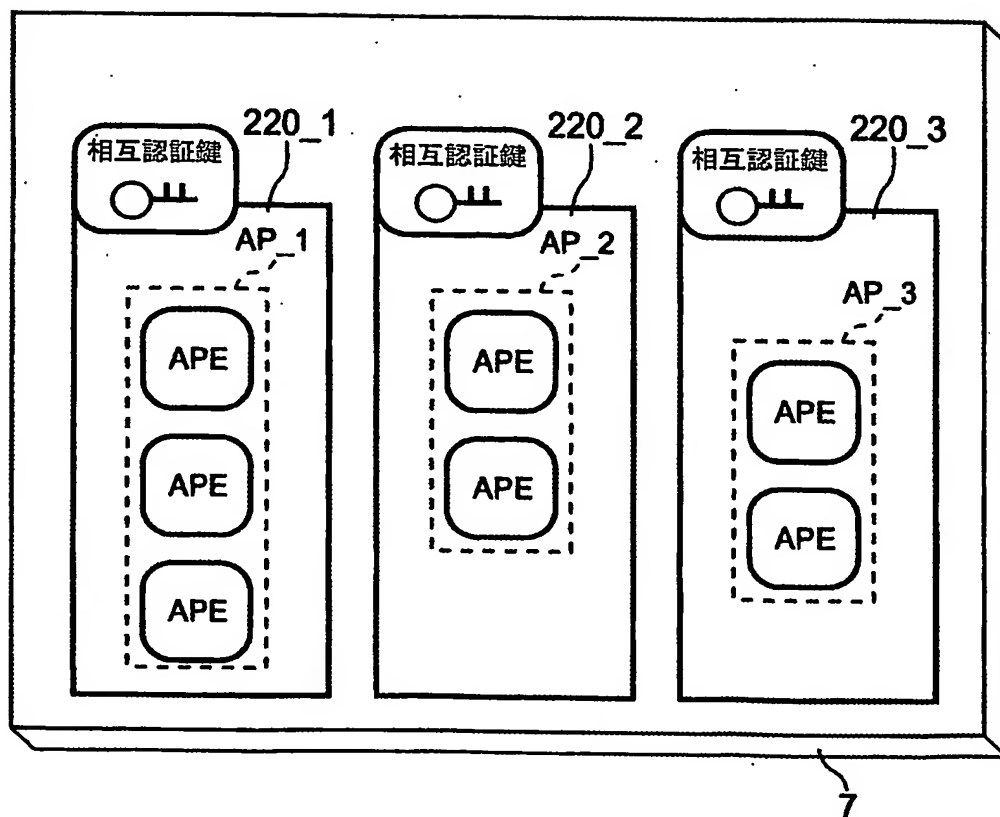


FIG. 10

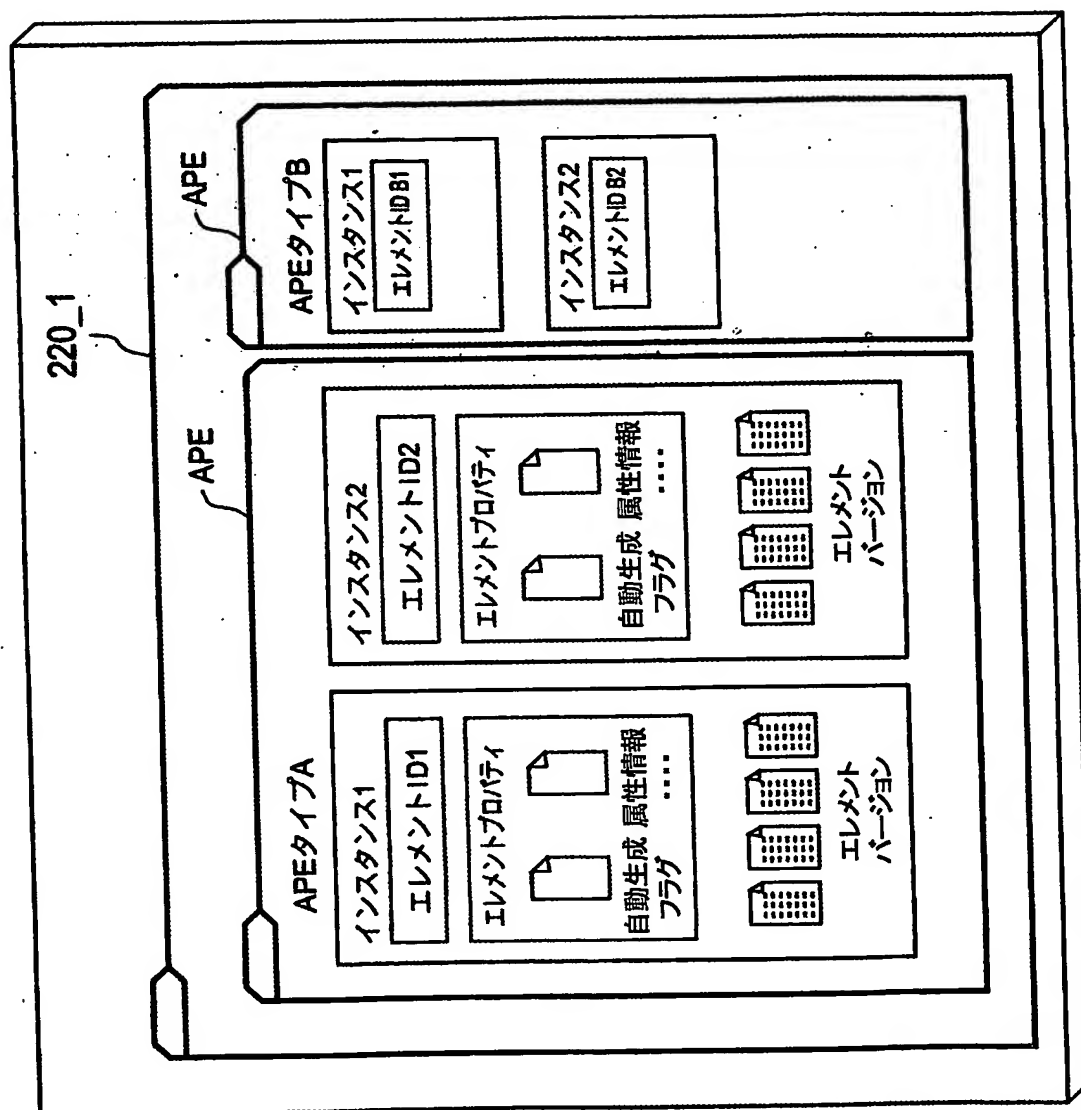


FIG. 11

APE タイプ番号	APEタイプ
...	ICシステム鍵
...	ICエリア鍵
...	ICサービス鍵
...	IC縮退鍵
...	IC鍵変更パッケージ
...	IC発行鍵パッケージ
...	IC拡張発行鍵パッケージ
...	ICエリア登録鍵パッケージ
...	ICエリア削除鍵パッケージ
...	ICサービス登録鍵パッケージ
...	ICサービス削除鍵パッケージ
...	ICメモリ分割鍵パッケージ
...	ICメモリ分割素鍵パッケージ
...	障害記録ファイル
...	相互認証用鍵
...	パッケージ鍵
...	ネガリスト
...	サービスデータテンポラリファイル

FIG. 12

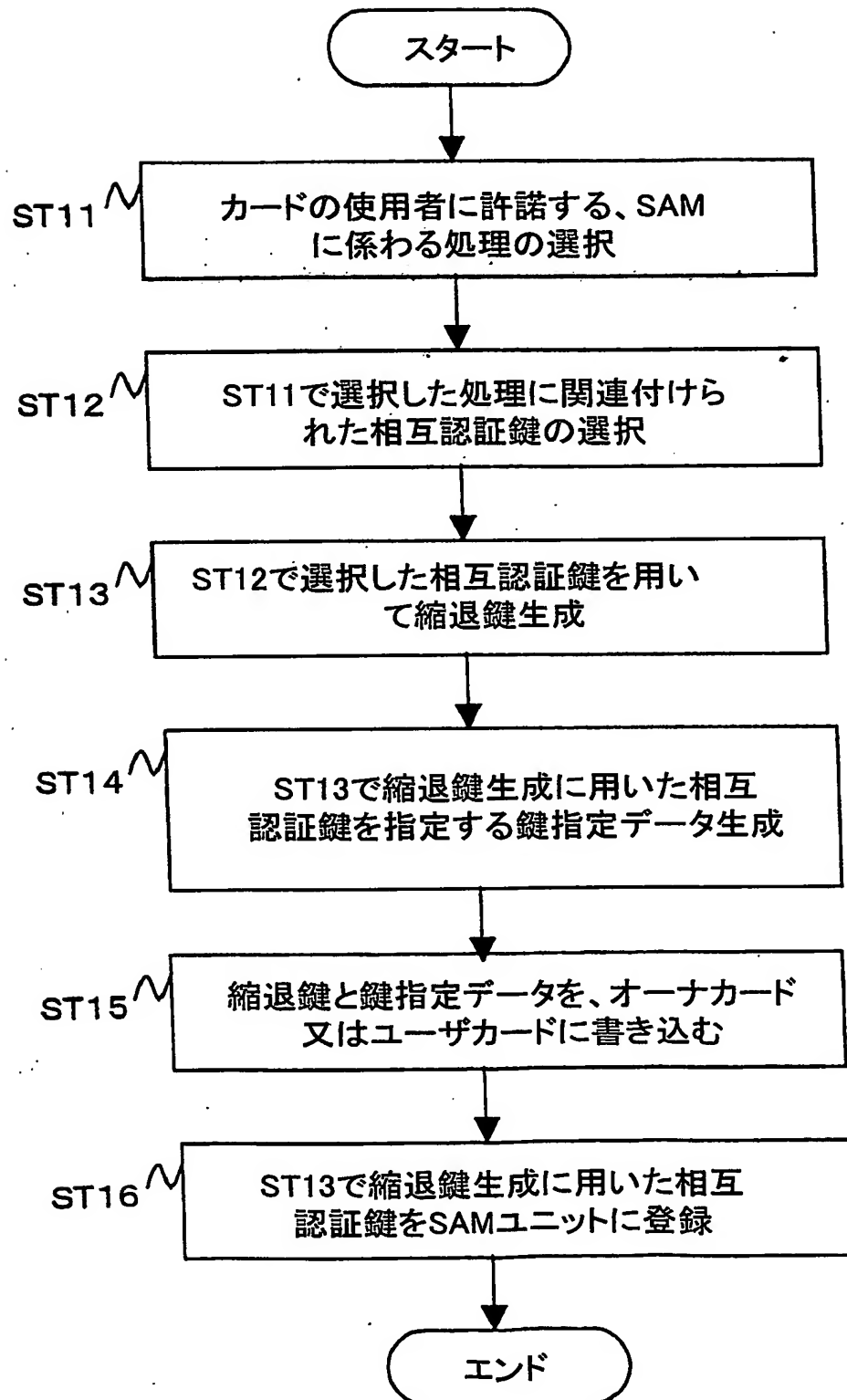


FIG. 13

相互認証鍵名	AP記憶領域・ID	APEタイプ 番号	インスタンス 番号	エレメント バージョン
デバイス鍵
ターミネーション鍵
製造設定サービス相互認証鍵
機器管理サービス相互認証鍵
通信管理サービス相互認証鍵
相互認証サービス相互認証鍵
AP記憶領域管理サービス 相互認証鍵
サービスAP・記憶領域 相互認証鍵
システムAP・記憶領域 相互認証鍵
製造者AP記憶領域 相互認証鍵

FIG. 14

AP記憶領域ID	エレメントタイプ番号	エレメント インスタンス番号	エレメント バージョン番号
2バイト	2バイト	2バイト	2バイト
所属する APIソース領域	相互認証鍵(固定値)	リリース鍵リングのID	使用する鍵の バージョン番号

FIG. 15A

相互認証鍵名	AP記憶領域ID	APE タイプ番号	インスタンス 番号	エレメント バージョン番号
デバイス鍵
機器管理サービス相互認証鍵
通信管理サービス相互認証鍵
AP記憶領域管理 サービス相互認証鍵
サービスAP記憶領域 AP-R相互認証鍵
ターミネーション鍵

・実行可能なコマンド

FIG. 15B

サービス種別	コマンド名
機器管理サービス	...
通信管理サービス	...
ICサービス	...
相互認証サービス	...
AP記憶領域管理サービス	...

FIG. 16

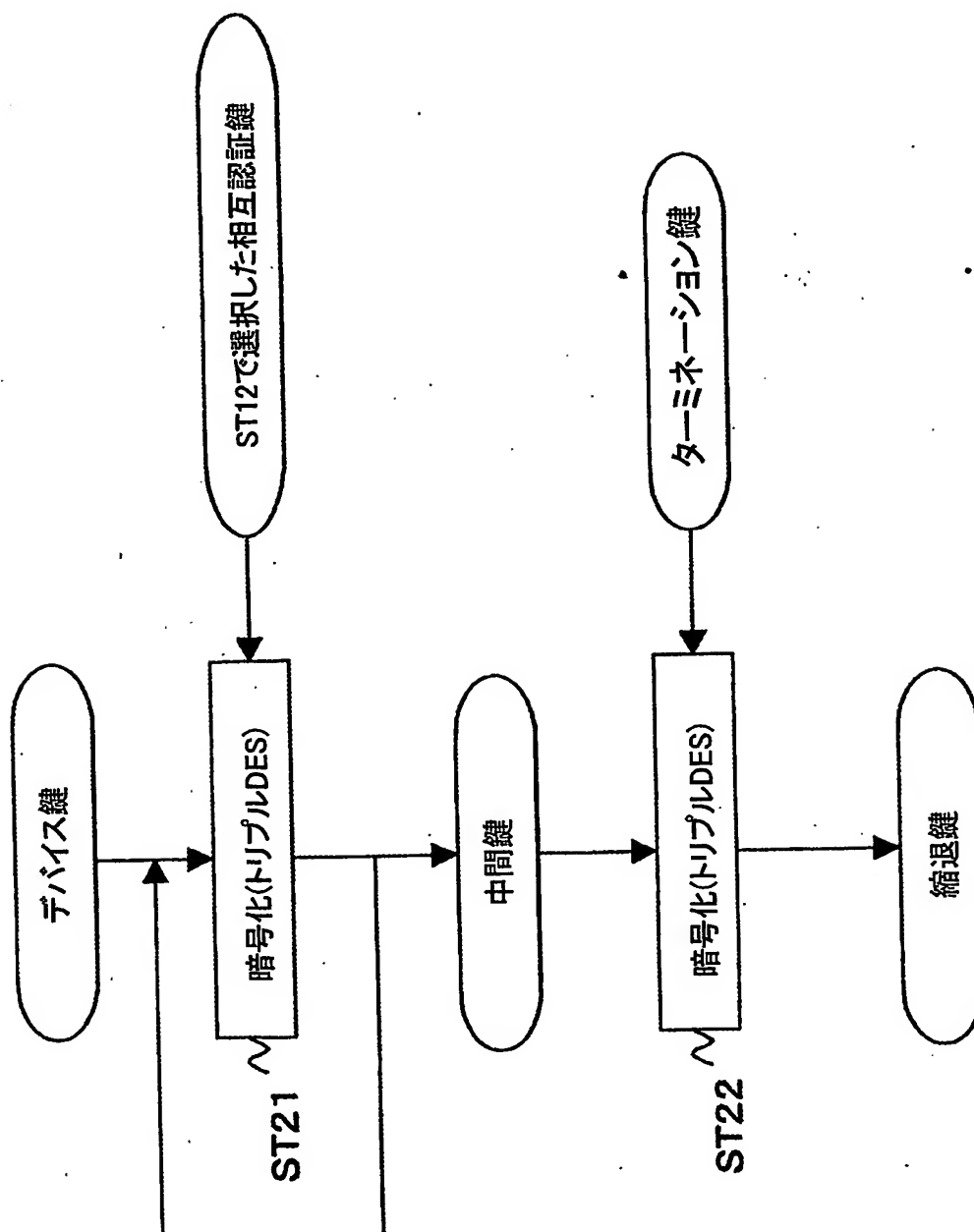


FIG. 17

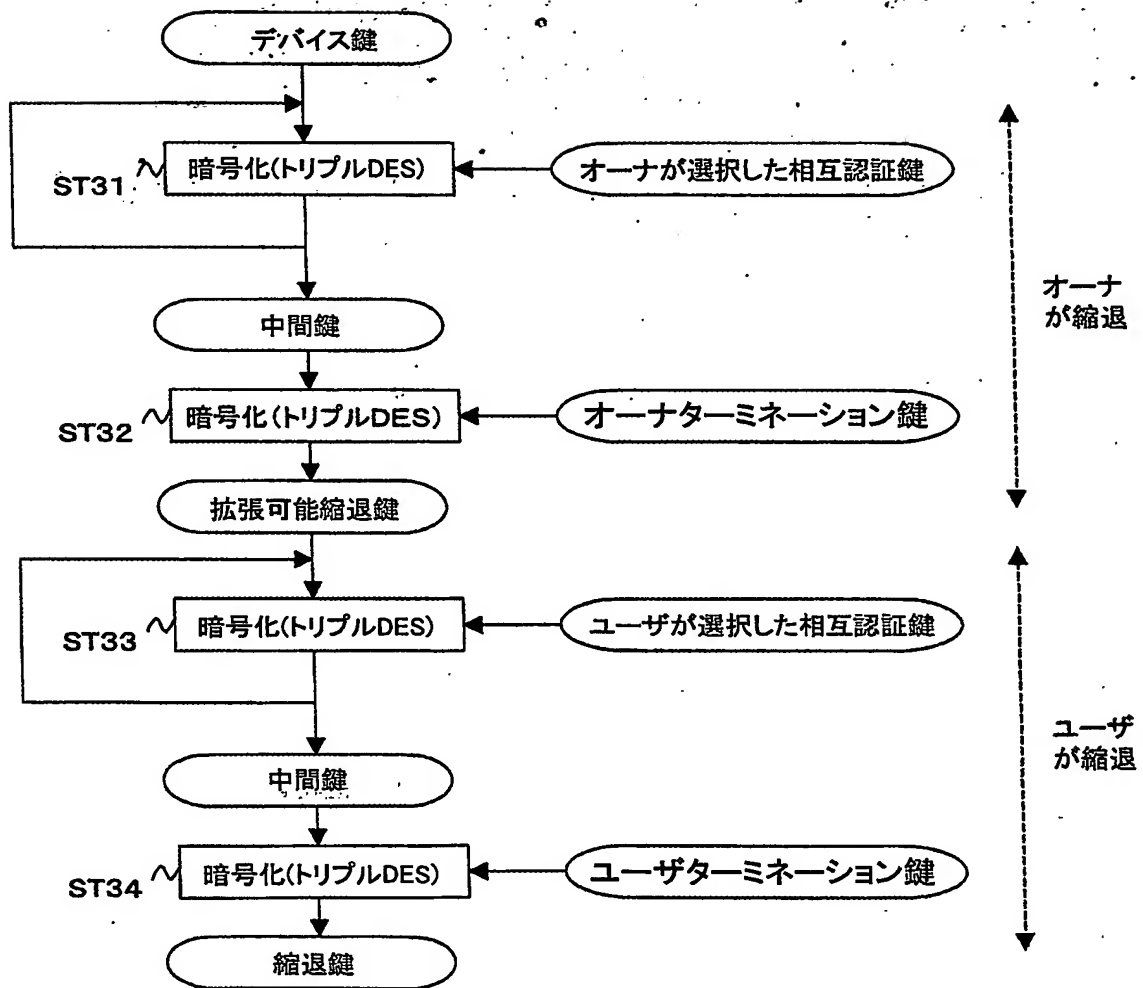


FIG. 18

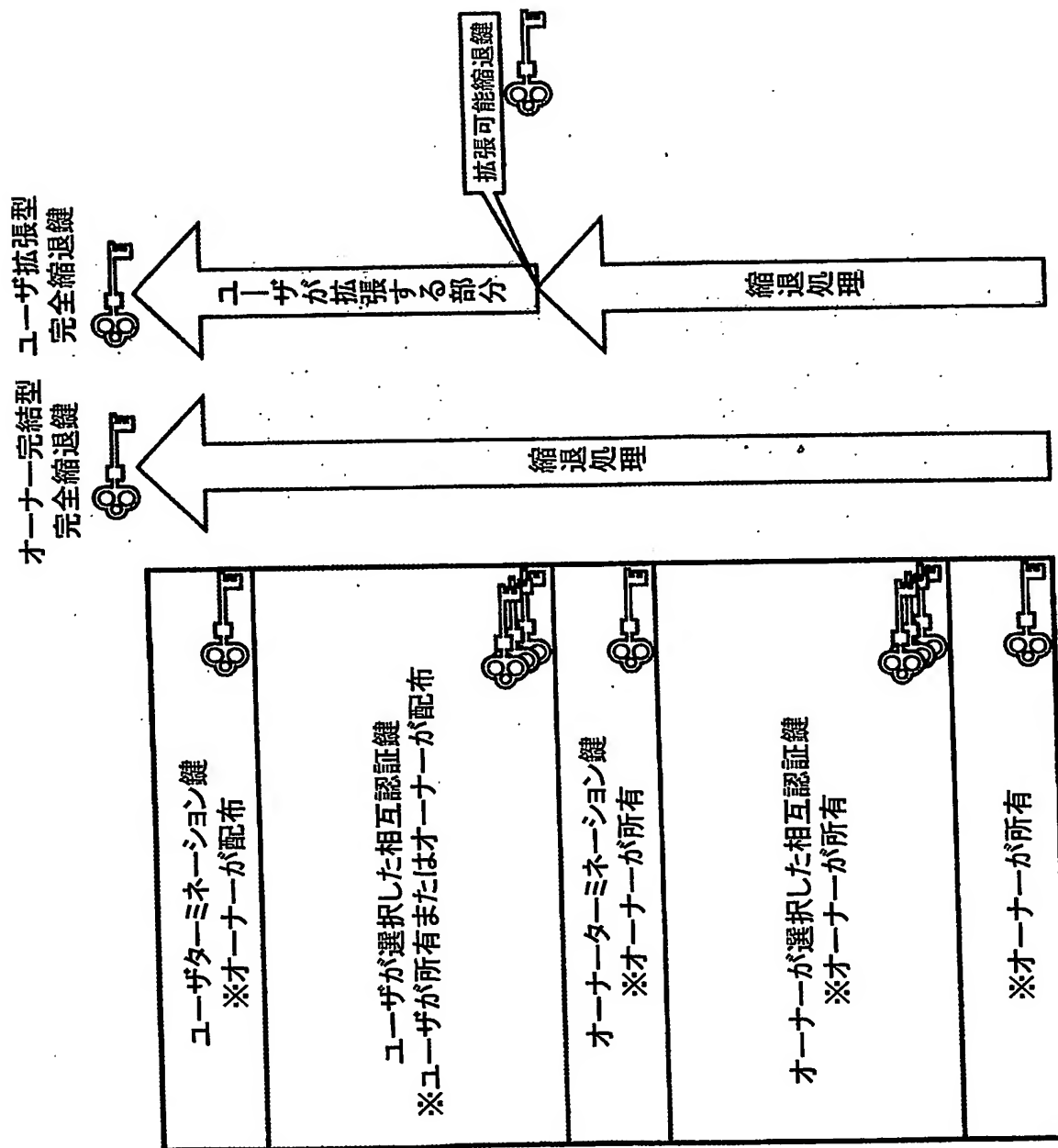


FIG. 19

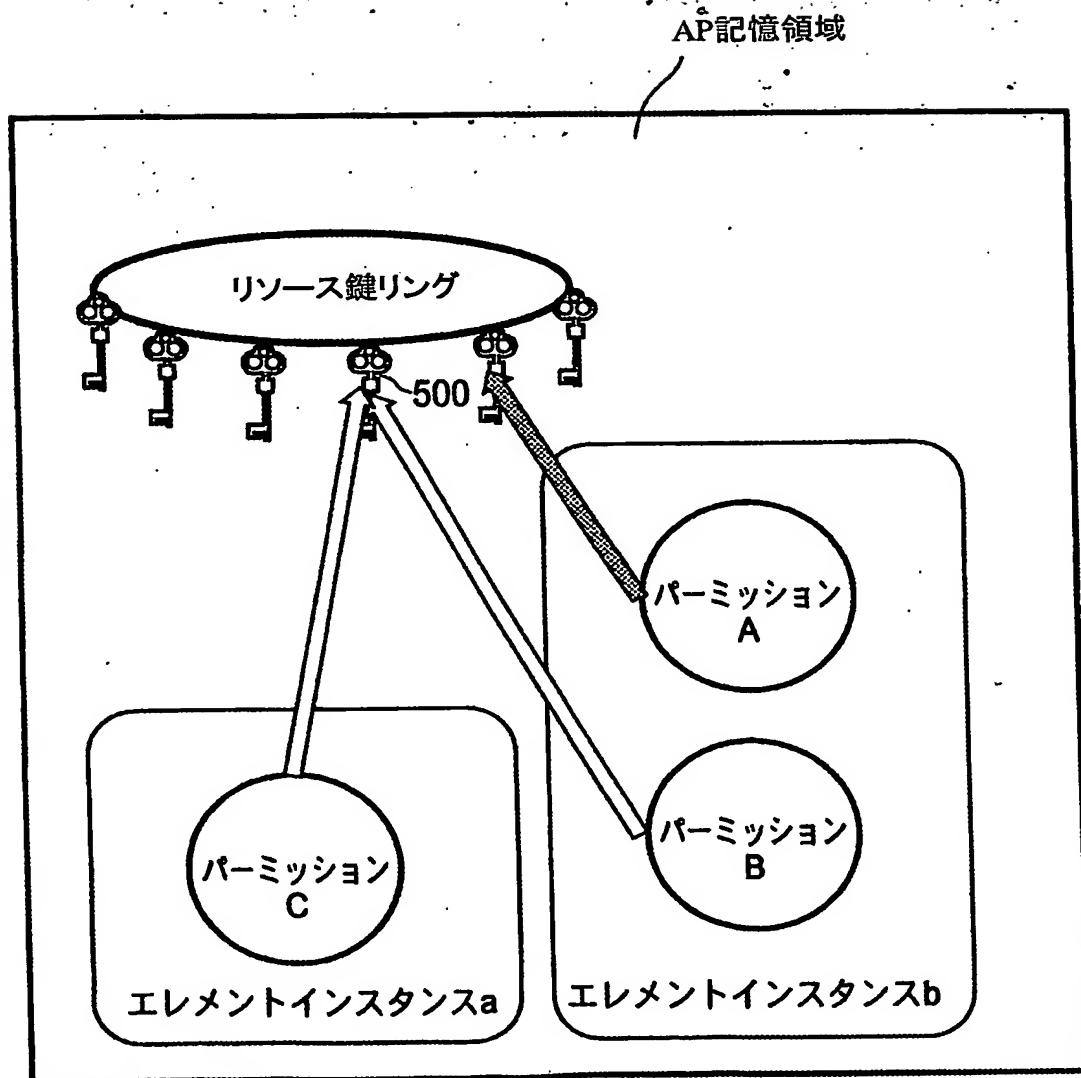


FIG. 20

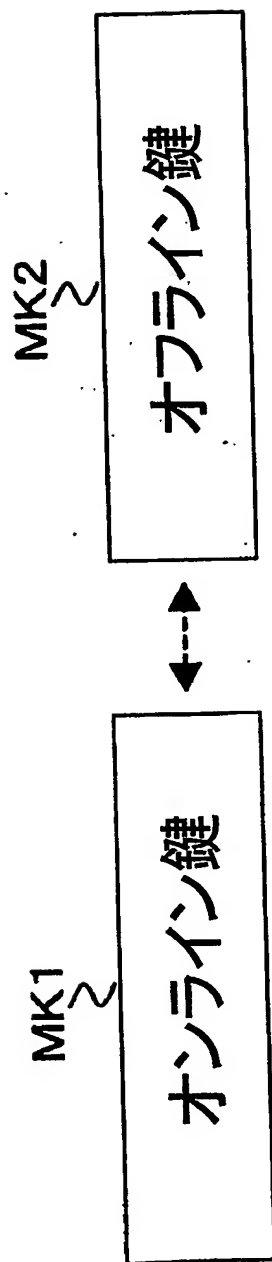


FIG. 21

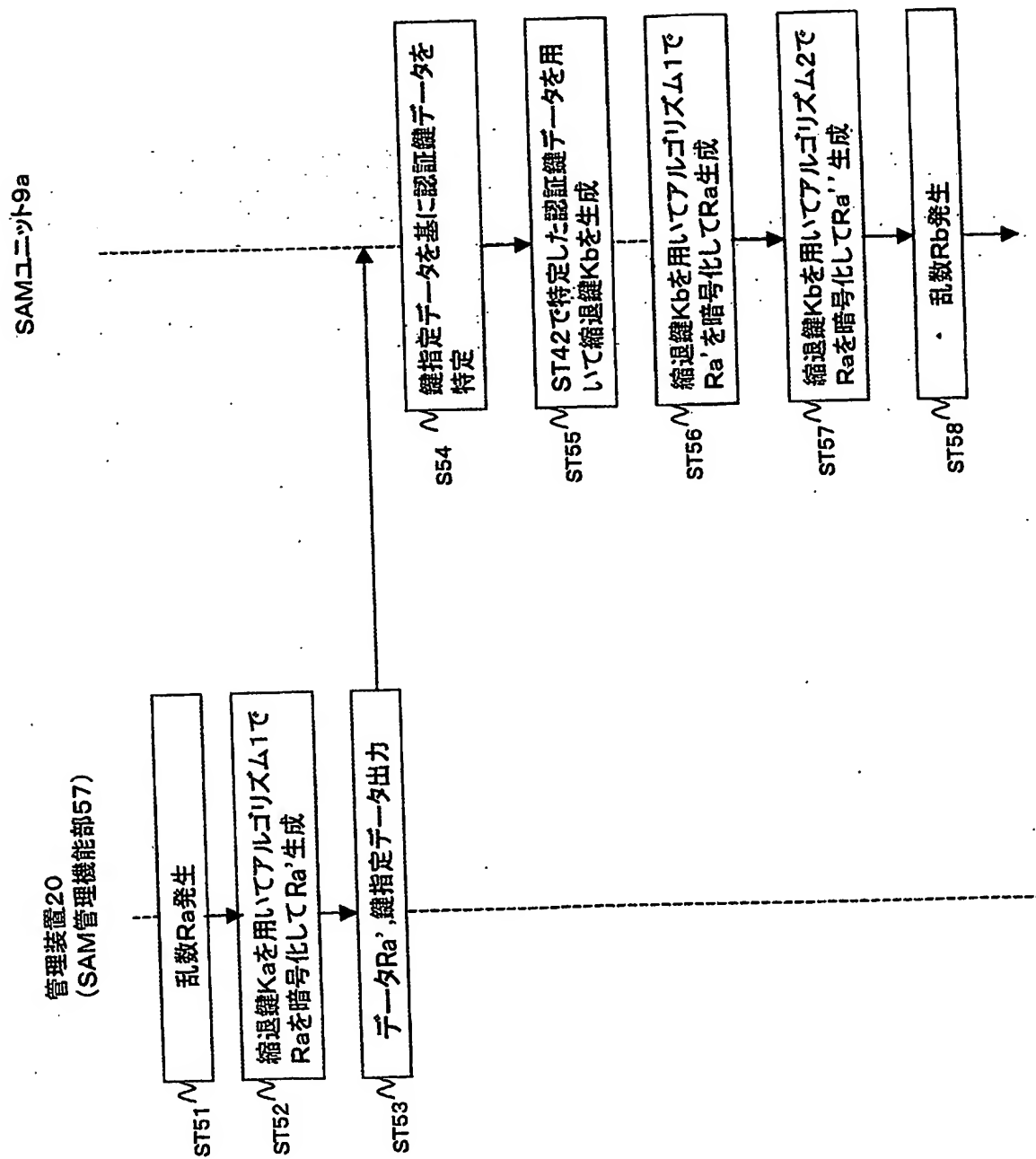


FIG. 22

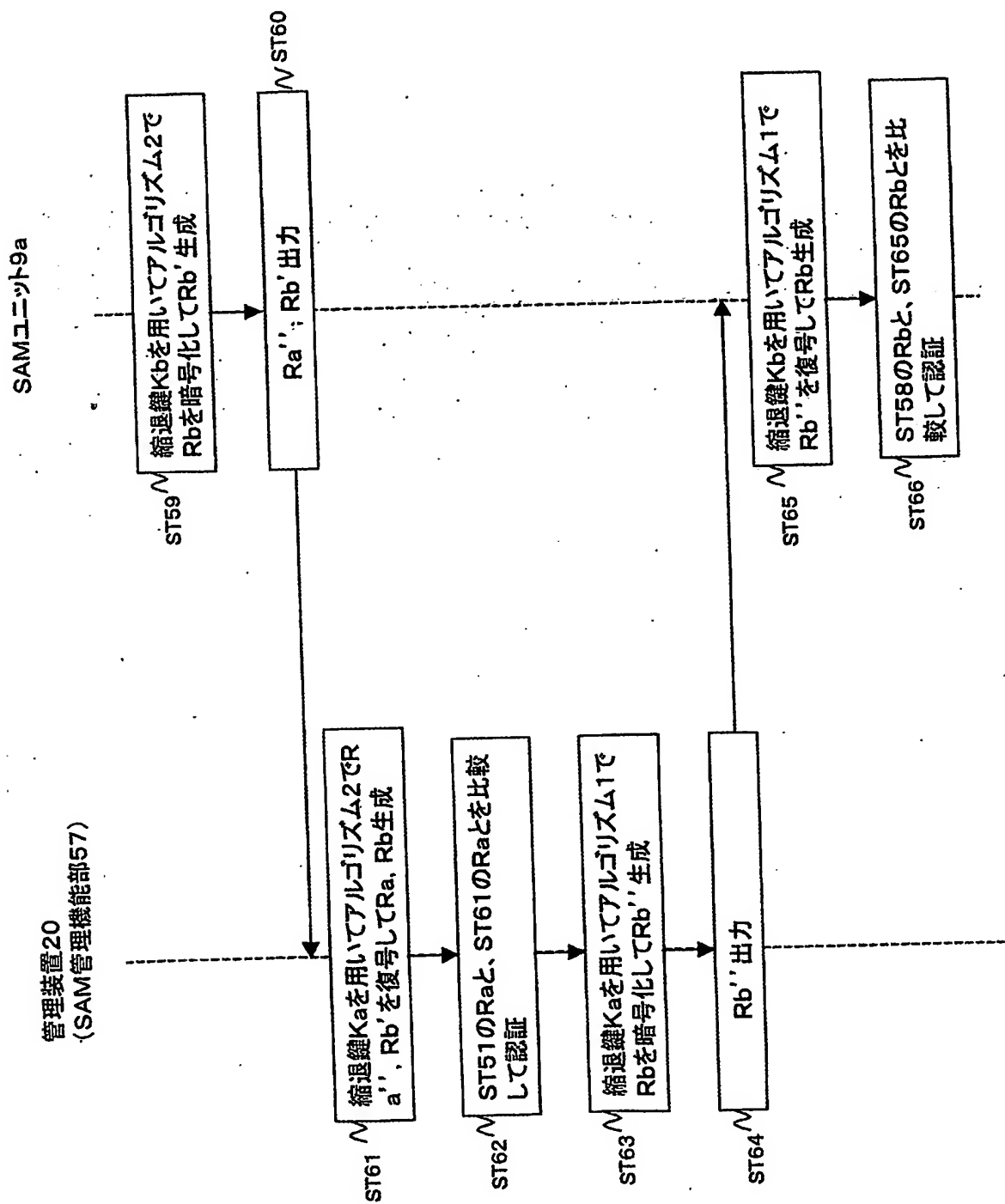


FIG. 23

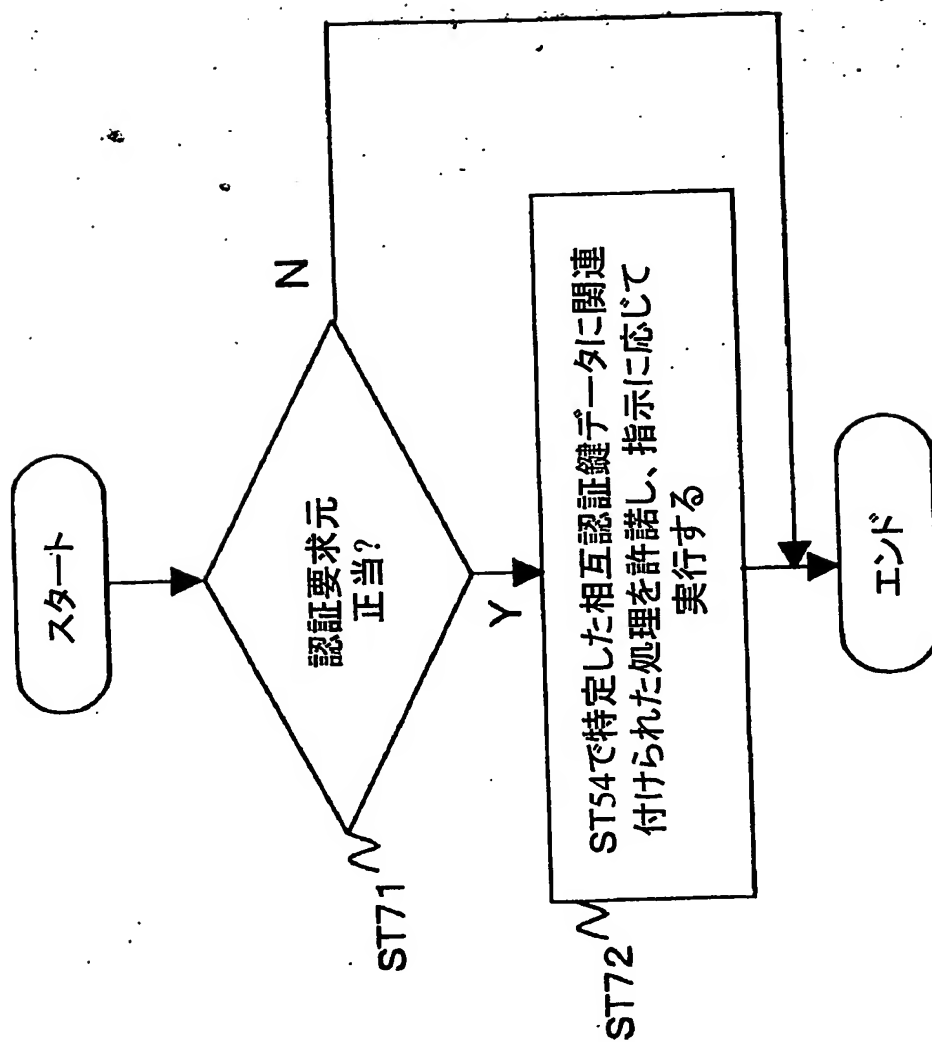


FIG. 24

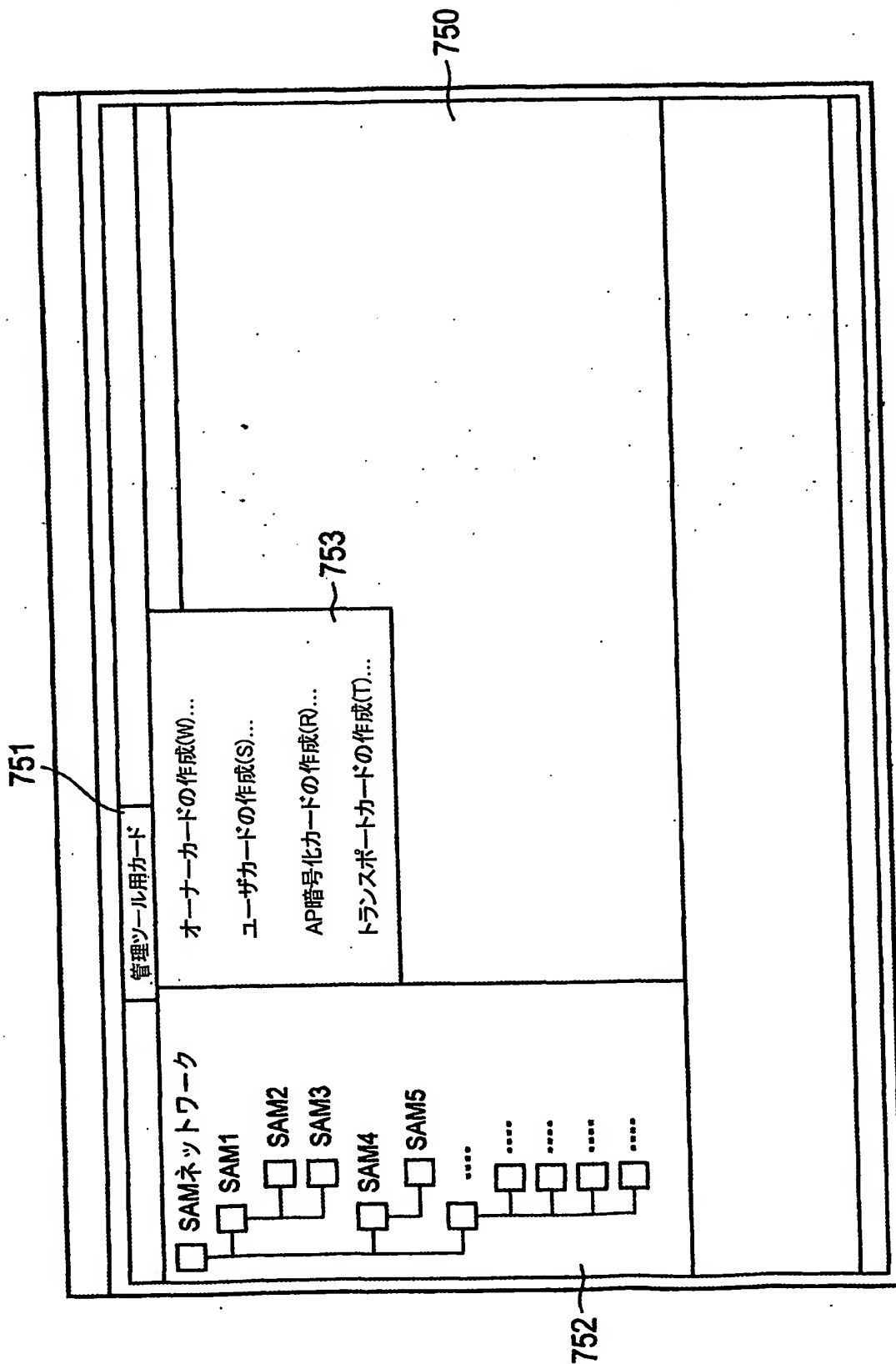


FIG. 25

オーナーカードの作成

利用サービスの選択

<input checked="" type="checkbox"/> 機器管理サービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/> 通信管理サービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/> 相互認証サービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/> APIソース領域管理サービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/> ログ記録サービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/> ネガリストサービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>

サービスAP記憶領域

<input checked="" type="checkbox"/> 読み取り	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/> 書き取り	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/> パッケージ	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>

システムAP記憶領域

<input checked="" type="checkbox"/> 読み取り	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/> 書き取り	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/> パッケージ	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>

デバイス/ターミネーション鍵

<input checked="" type="checkbox"/> デバイス鍵	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/> ターミネーション鍵	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>

OK

キャンセル

24/45

FIG. 26

○○○カードを作成します

○○○カードをリーダー/ライターにセットして下さい。

作成 キャンセル

770

771

The image shows a rectangular dialog box with a title bar at the top containing the text '○○○カードを作成します'. Below the title bar is a large text area containing the instruction '○○○カードをリーダー/ライターにセットして下さい。'. At the bottom of the dialog box are two buttons: '作成' (Create) on the left and 'キャンセル' (Cancel) on the right. A bracket labeled '770' points to the right side of the dialog box, and a bracket labeled '771' points to the bottom of the dialog box.

FIG. 27

ユーザカードの作成

利用サービスの選択

<input type="checkbox"/>	機器管理サービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/>	通信管理サービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/>	相互認証サービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/>	APIリソース領域管理サービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input type="checkbox"/>	ログ記録サービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input type="checkbox"/>	ネガリストサービス	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>

サービスAP記憶領域

<input type="checkbox"/>	読み取り	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input type="checkbox"/>	書き取り	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/>	パッケージ	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>

システムAP記憶領域

<input checked="" type="checkbox"/>	読み取り	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/>	書き取り	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/>	パッケージ	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>

デバイス/ターミネーション鍵

<input checked="" type="checkbox"/>	デバイス鍵	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>
<input checked="" type="checkbox"/>	ターミネーション鍵	鍵バージョン:	<div style="border: 1px solid black; padding: 2px; text-align: center;">0x0001 ▼</div>

OK

キャンセル

FIG. 28

APIソース暗号化カードの作成

利用サービスの選択

<input checked="" type="checkbox"/> 機器管理サービス	鍵バージョン: <input type="text" value="0x0001"/>
<input checked="" type="checkbox"/> 通信管理サービス	鍵バージョン: <input type="text" value="0x0001"/>
<input checked="" type="checkbox"/> 相互認証サービス	鍵バージョン: <input type="text" value="0x0001"/>
<input checked="" type="checkbox"/> APIソース領域管理サービス	鍵バージョン: <input type="text" value="0x0001"/>
<input checked="" type="checkbox"/> ログ記録サービス	鍵バージョン: <input type="text" value="0x0001"/>
<input checked="" type="checkbox"/> ネガリストサービス	鍵バージョン: <input type="text" value="0x0001"/>

サービスAP記憶領域

<input checked="" type="checkbox"/> 読み取り	鍵バージョン: <input type="text" value="0x000"/>
<input checked="" type="checkbox"/> 書き取り	鍵バージョン: <input type="text" value="0x000"/>
<input checked="" type="checkbox"/> パッケージ	鍵バージョン: <input type="text" value="0x0001"/>

システムAP記憶領域

<input checked="" type="checkbox"/> 読み取り	鍵バージョン: <input type="text" value=""/>
<input checked="" type="checkbox"/> 書き取り	鍵バージョン: <input type="text" value=""/>
<input checked="" type="checkbox"/> パッケージ	鍵バージョン: <input type="text" value=""/>

デバイス/ターミネーション鍵

<input checked="" type="checkbox"/> デバイス鍵	鍵バージョン: <input type="text" value=""/>
<input checked="" type="checkbox"/> ターミネーション鍵	鍵バージョン: <input type="text" value=""/>

OK

キャンセル

27/45

FIG. 29

800

トランスポートカードの作成

次のAPIリソースエレメントを読み出します。

SAM IPアドレス:

AP記憶領域: サービス領域 ▼

エレメントタイプ: IC分割鍵 ▼

インスタンス番号: 0000h ▼

バージョン: 0000h ▼

OK キャンセル

FIG. 30

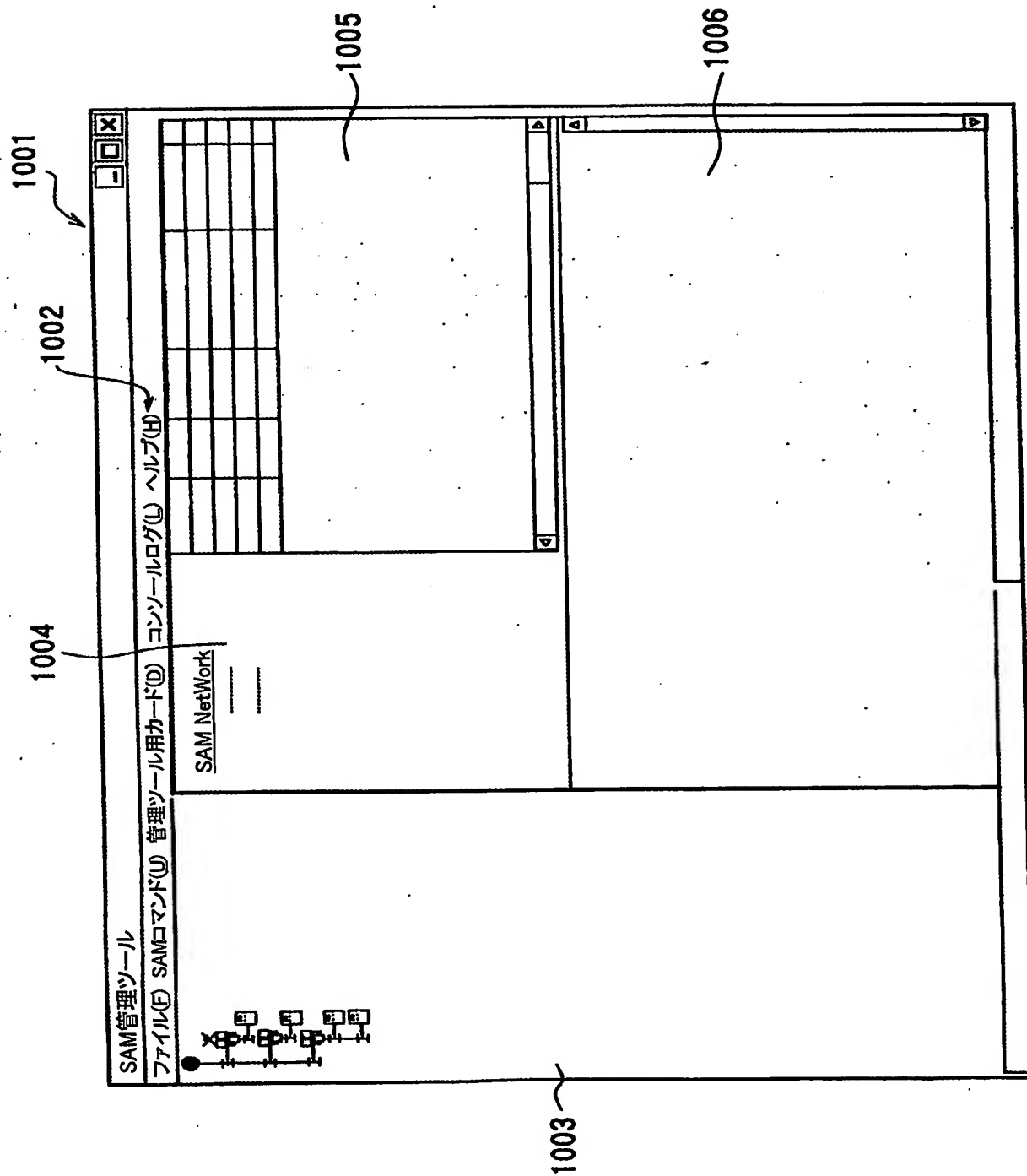


FIG. 31

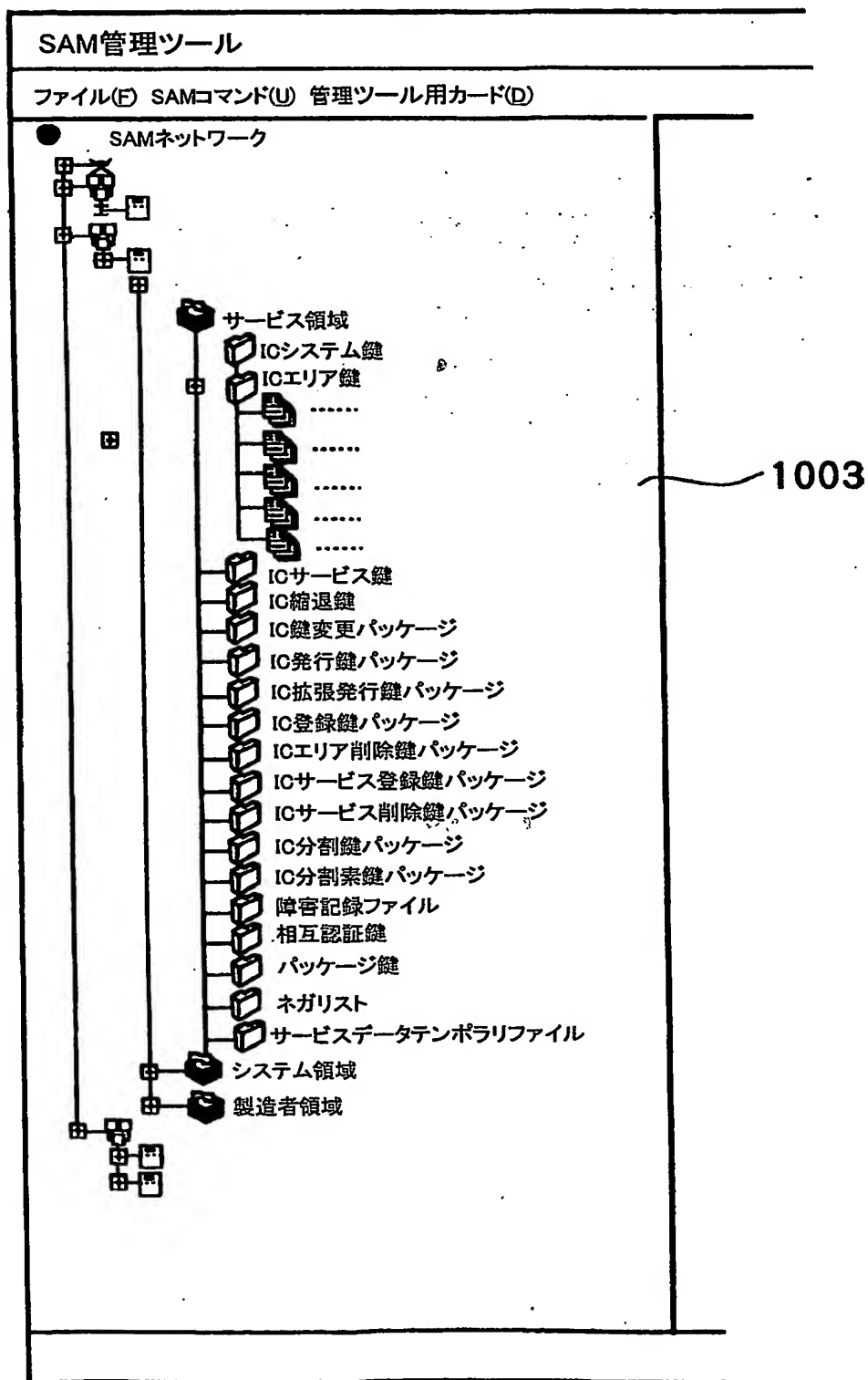


FIG. 32

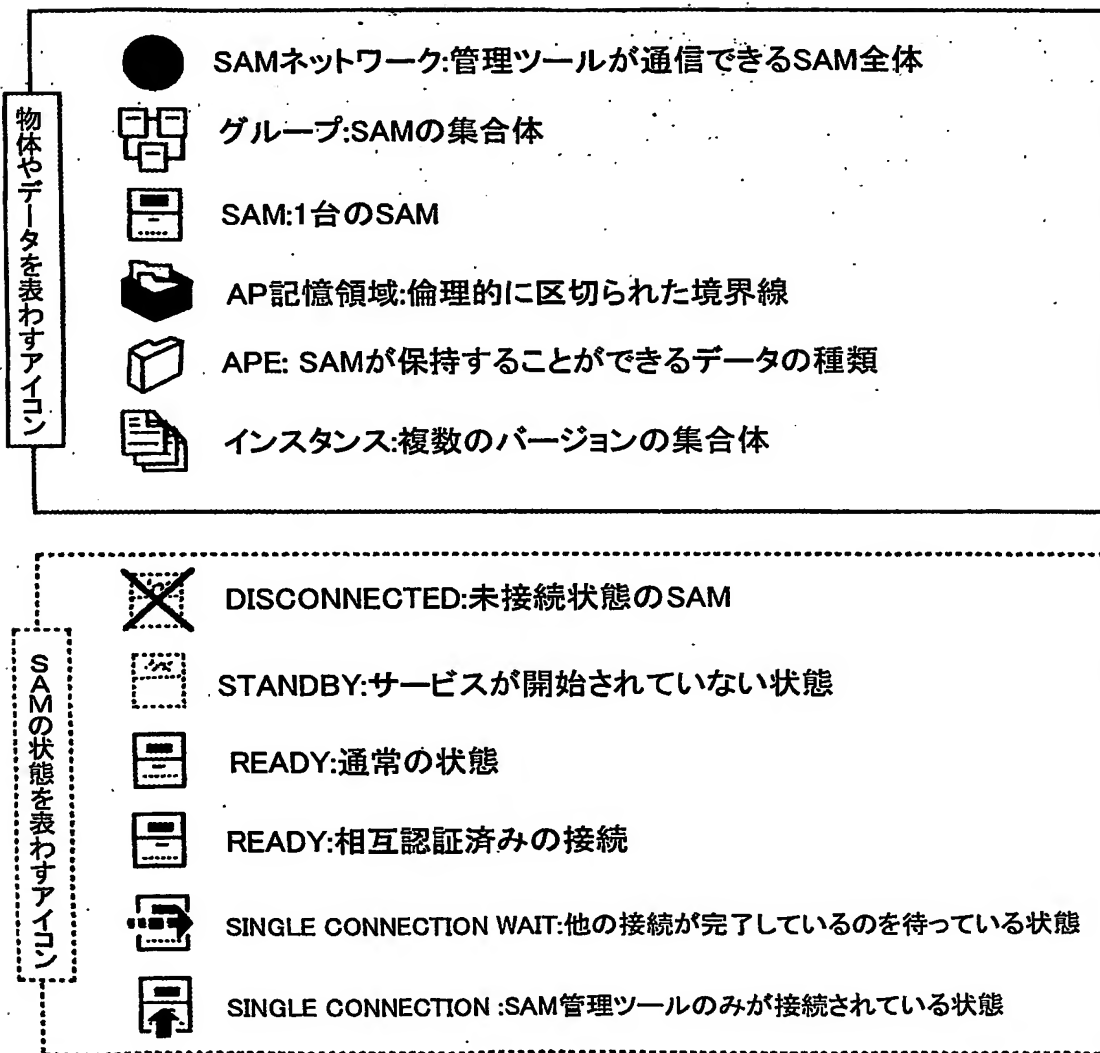


FIG. 33

コンソールログ(L) ヘルプ(H)					
SAM Network					
IPアドレス	ポート	種類	状態	SAM Name	コメント
.....	SAM			
		グループ			
		グループ			
		グループ			

1010

FIG. 34

コンソールログ(L) ヘルプ(H)

IPアドレス	ポート	種類	状態	SAM Name	コメント
.....	SAM	READY		

Group

1020

FIG. 35

コンソールログ(L) ヘルプ(H)

記憶領域	種類	用途
.....	AP記憶領域	サービス領域
.....	AP記憶領域	システム領域
.....	AP記憶領域	製造者領域

SAM

READYモード

1030

FIG. 36

AP Resource Partition	
サービス領域	
APEタイプ番号	APEタイプ
.....	システム鍵
.....	ICエリア鍵
.....	ICサービス鍵
.....	IC縮退鍵
.....	IC鍵変更パッケージ
.....	IC発行鍵パッケージ
.....	IC拡張発行鍵パッケージ
.....	IC登録鍵パッケージ
.....	ICエリア削除鍵パッケージ
.....	ICサービス登録鍵パッケージ
.....	ICサービス削除鍵パッケージ
.....	IC分割鍵パッケージ
.....	IC分割素鍵パッケージ
.....	障害記録ファイル
.....	相互認証鍵
.....	パッケージ鍵
.....	ネガリスト
.....	サービスデータテンポラリファイル

1040

FIG. 38

Instance

.....

SAM-EVT-33

....., jp

READYモード

サービズ領域

ICサービズ鍵

インスタンス番号.....

最大Ver数.....

使用Ver.....

最小Ver数.....

最大Ver数.....

タグ.....

自動生成しない

エレメント取得可能

削除可能

システムコード.....

サービズコード.....

現エリアコード.....

1060

FIG. 39

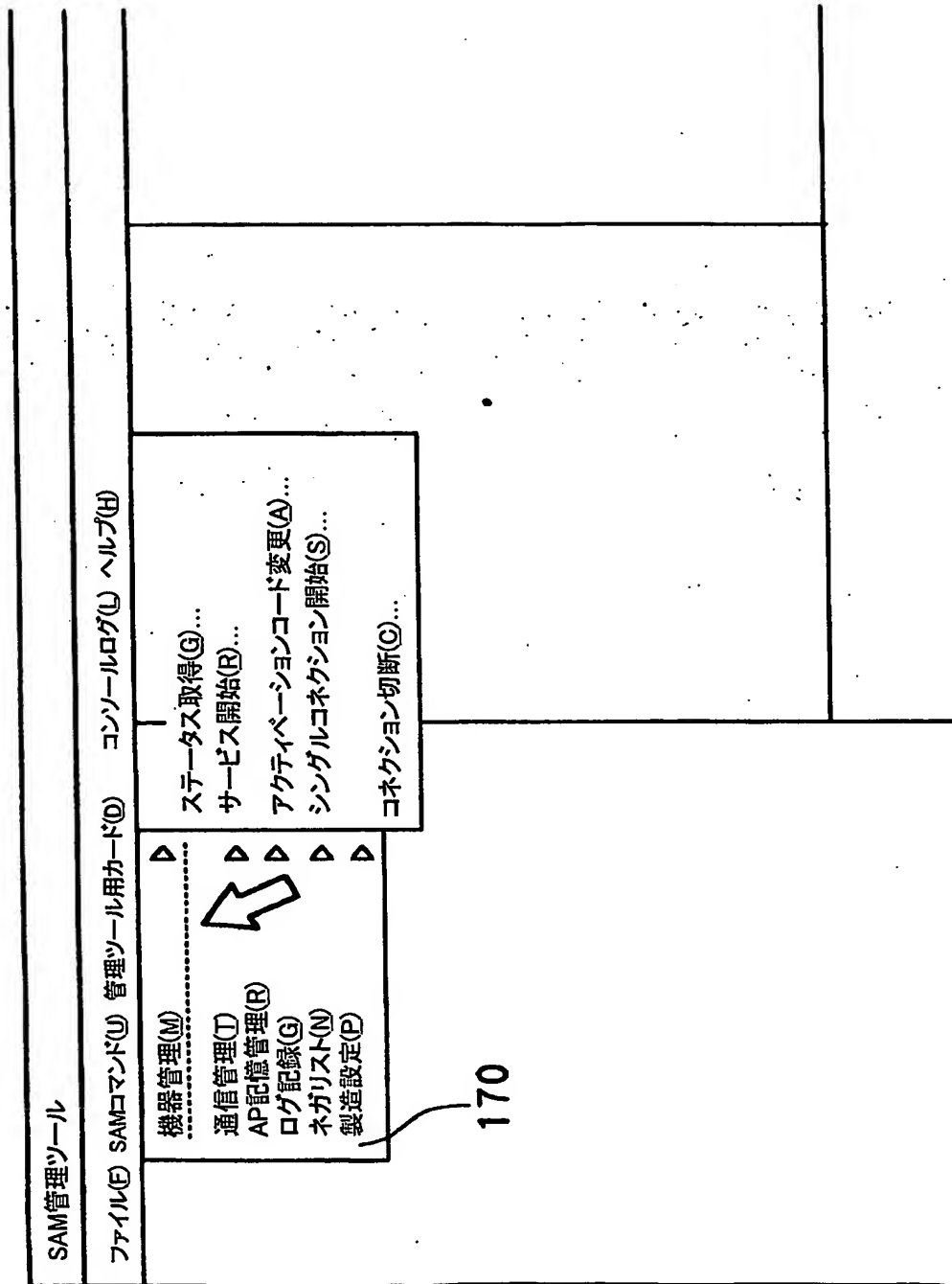


FIG. 40

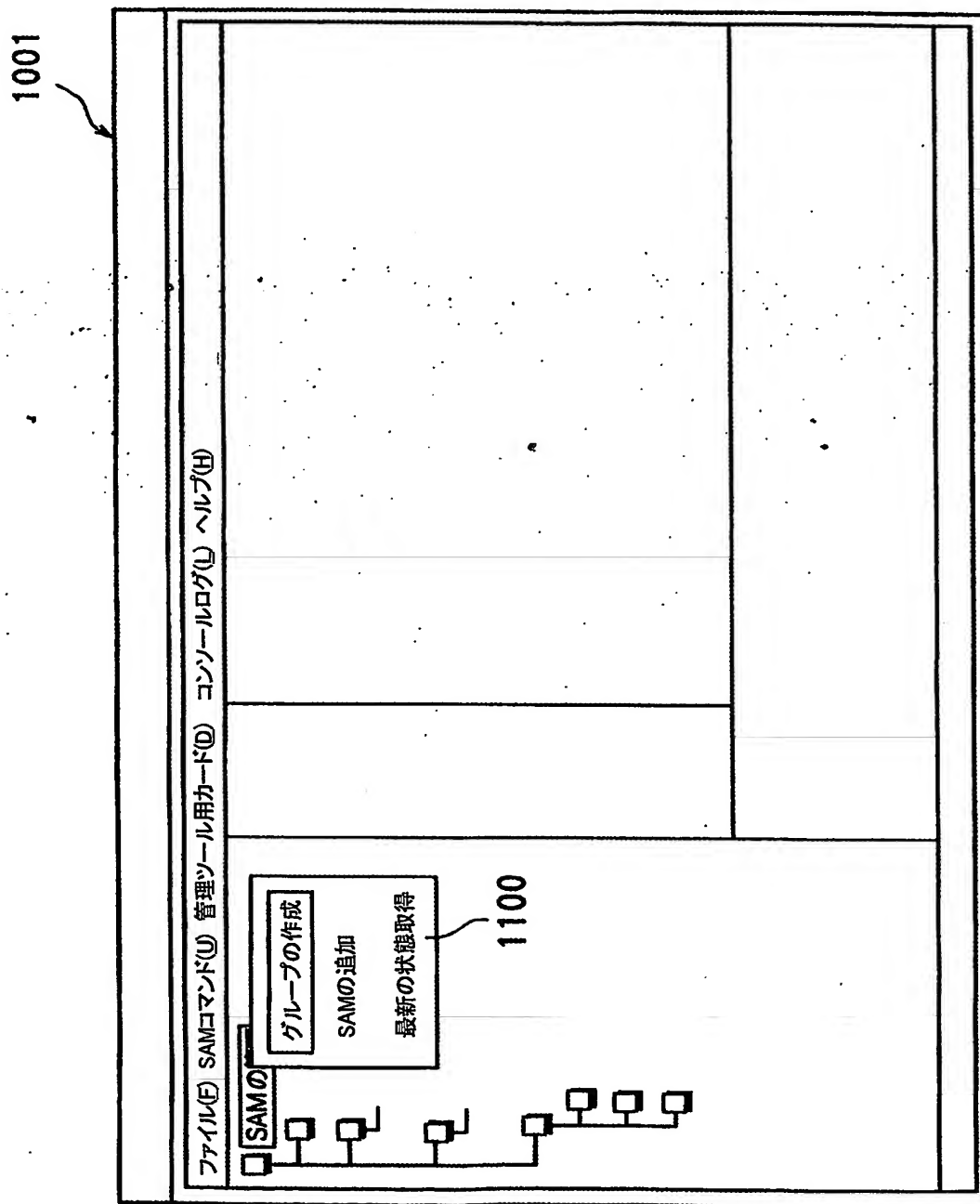


FIG. 41

1210 1220 1230

□ AP記憶領域エディタ

ファイル(F) ヘルプ(H)

AP記憶領域:

エレメントパッケージリスト

追加... 削除 編集...

パッケージタイプ	エレメントタイプ	インスタント番号

1200

FIG. 42

エレメントパッケージの追加

エレメントパッケージタイプ

☒ エレメント作成 1301

☐ パッケージ追加

APEタイプ : 1302

ICシステム鍵

インスタンス番号 : 1303

ファイル... 1304

OK

キャンセル

1300

FIG. 43

APE作成

エレメントタイプ: ICシステム鍵 インスタンス番号:

タグ: 1401

使用バージョン数: 20 1402

データ自動生成: 可 1404

エレメント取得: 可 1405

属性情報

属性情報名	値
システムコード

カード参照...

属性編集... 保存 キャンセル

1406

FIG. 44

APEバージョン追加

エレメントタイプ: IC鍵変更パッケージ

インスタンス番号 :

エレメントバージョン:

鍵データ入力方法: 手動 ▽

エレメントデータ

カード参照...

項目名	値
IC鍵変更パッケージ	XXX...

属性編集...

保存

キャンセル

43/45

FIG. 45

□ AP記憶領域エディタ

ファイル(E) ヘルプ(H)

AP記憶領域: サービス領域

エレメントパッケージリスト

追加...

削除

編集...

	パッケージタイプ	エレメントタイプ	インスタント番号
1	エレメント作成	ICサービス鍵
2	バージョン追加	ICサービス鍵
3	エレメント作成	ICサービス鍵
4	バージョン追加	ICサービス鍵

120

1240

符号の説明

- 1…通信システム
- 2…サーバ装置
- 3…I Cカード
- 4…カードRW
- 6…P C
- 7…外部メモリ
- 8…SAMモジュール
- 9 a, 9 b…SAMユニット
- 19 a, 19 b…ASPサーバ装置
- 20…管理装置
- 51…AP編集ツール
- 52…管理ツール
- 53…カードリーダー・ライタ
- 54…ディスプレイ
- 55…I/F、56…操作部
- 57…SAM管理機能部
- 58…カード管理機能部
- 61…メモリI/F
- 62…外部I/F
- 63…メモリ
- 64…認証部
- 65…CPU
- 71…デフォルトカード
- 72…オーナーカード
- 73…ユーザカード
- 74…トランスポートカード
- 75…AP暗号化カード

INTERNATIONAL SEARCH REPORT

International application No.
JP/JP03/11802

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ H04L9/32, H04L9/08, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ H04L9/32, H04L9/08, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 11-163853 A (KDD Kabushiki Kaisha), 18 June, 1999 (18.06.99), Par. Nos. [0021] to [0035]; Figs. 1 to 5 Par. Nos. [0021] to [0035]; Figs. 1 to 5 (Family: none)	1-15, 19, 20 16-18
Y	JP 11-102471 A (NTT Data Corp.), 13 April, 1999 (13.04.99), Par. Nos. [0057] to [0068]; Figs. 1, 4, 6, 7 (Family: none)	16
Y	JP 6-261034 A (NTT Data Communications Systems Corp.), 16 September, 1994 (16.09.94), Par. Nos. [0011]; Figs. 2, 4 (Family: none)	17, 18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>
--	---

Date of the actual completion of the international search
12 December, 2003 (12.12.03)

Date of mailing of the international search report
24 December, 2003 (24.12.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁷ H04L9/32 H04L9/08 G06F15/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁷ H04L9/32 H04L9/08 G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2003年
 日本国登録実用新案公報 1994-2003年
 日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	JP 11-163853 A (ケイディディ株式会社) 1999.06.18 第【0021】-【0035】段落, 図1-5 第【0021】-【0035】段落, 図1-5 (ファミリーなし)	1-15, 19, 20 16-18
Y	JP 11-102471 A (株式会社エヌ・ティ・ティ・データ) 1999.04.13 第【0057】-【0068】段落, 図1, 4, 6, 7 (ファミリーなし)	16

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に関する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

12.12.03

国際調査報告の発送日

24.12.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)
 青木 重徳



5M 4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 6-261034 A (エヌ・ティ・ティ・データ通信株式会社) 1994. 09. 16 第【0011】段落, 図2, 4 (ファミリーなし)	17, 18